

PRIRUČNIK

Priručnik o europskom zakonodavstvu o zaštiti podataka

Izdanje iz 2018.



Rukopis ovoga priručnika završen je u travnju 2018.

Ažurirane verzije ubuduće će biti na raspolaganju na internetskoj stranici Agencije Europske unije za temeljna prava (FRA) na adresi fra.europa.eu, na internetskoj stranici Vijeća Europe na adresi coe.int/dataprotection, na internetskoj stranici Europskog suda za ljudska prava na adresi echr.coe.int, u izborniku *Case-law* (Sudska praksa), te na internetskoj stranici Europskog nadzornika za zaštitu podataka na adresi edps.europa.eu

Fotografija (naslovnica i unutrašnjost): © iStockphoto

© Agencija Europske unije za temeljna prava i Vijeće Europe, 2020.

Umnožavanje je dopušteno uz uvjet navođenja izvora.

Za svaku uporabu ili reprodukciju fotografija ili drugog materijala koji nije zaštićen autorskim pravom Agencije Europske unije za temeljna prava/Vijeća Europe potrebno je tražiti dopuštenje izravno od nositelja autorskih prava.

Ni Agencija Europske unije za temeljna prava/Vijeće Europe ni bilo koja osoba koja djeluje u ime Agencije Europske unije za temeljna prava/Vijeća Europe ne odgovara za moguću upotrebu informacija u nastavku.

Dodatne informacije o Europskoj uniji dostupne su na internetu (<http://europa.eu>).

Luksembourg: Ured za publikacije Europske unije, 2020.

Vijeće Europe: ISBN 978-92-871-9835-8

FRA – print: ISBN 978-92-9474-443-2

FRA – PDF: ISBN 978-92-9474-442-5

doi:10.2811/266278

doi:10.2811/66223

TK-05-17-225-HR-C

TK-05-17-225-HR-N

Priručnik je izvorno napisan na engleskom jeziku. Europski sud za ljudska prava (ESLJP) ne preuzima odgovornost za kvalitetu prijevoda na druge jezike. Stajališta iznesena u ovom priručniku nisu obvezujuća za ESLJP. Priručnik upućuje na nekoliko komentara i drugih priručnika. ESLJP ne snosi odgovornost za njihov sadržaj niti njihovo uključivanje na ovaj popis predstavlja bilo kakvu podršku tim publikacijama. Daljnje publikacije dostupne su na internetskim stranicama knjižnice ESLJP-a na adresi: echr.coe.int/Library

Sadržaj ovog priručnika ne predstavlja službeno stajalište Europskog nadzornika za zaštitu podataka (EDPS) i ne obvezuje ga u izvršavanju njegovih ovlasti. EDPS ne preuzima odgovornost za kvalitetu prijevoda na druge jezike.



Priručnik o europskom zakonodavstvu o zaštiti podataka

Izdanje iz 2018.

Predgovor

Naše je društvo sve više digitalizirano. Brzina tehnološkog razvoja i način obrade osobnih podataka svakodnevno utječu na svakoga od nas na različite načine s obzirom na promjene koje se odvijaju. Pravni okviri Europske unije (EU) i Vijeća Europe kojima se osigurava zaštita privatnosti i osobnih podataka nedavno su preispitani.

Europa ima jednu od vodećih uloga u zaštiti podataka na svjetskoj razini. Standardi zaštite podataka EU-a temelje se na Konvenciji br. 108 Vijeća Europe, instrumentima EU-a – uključujući Opću uredbu o zaštiti podataka i Direktivu o zaštiti podataka za policiju i tijela kaznenog pravosuđa – te na odgovarajućoj sudskoj praksi Europskog suda za ljudska prava i Suda Europske unije.

Reforme u području zaštite podataka koje su proveli EU i Vijeće Europe opsežne su i u nekim slučajevima složene, imaju širok raspon prednosti i utječu na pojedince i poduzeća. Cilj je ovoga priručnika podići svijest i doprinijeti boljem poznavanju propisa o zaštiti podataka, posebice među nespecijaliziranim pravnicima koji se u svojem radu susreću s problemima zaštite podataka.

Priručnik su izradili Agencija Europske unije za temeljna prava (FRA), Vijeće Europe (u suradnji s Registrom Europskog suda za ljudska prava) i Europski nadzornik za zaštitu podataka. Njime se ažurira izdanje iz 2014. i pripada seriji pravnih priručnika koje su zajednički izradili FRA i Vijeće Europe.

Želimo zahvaliti tijelima za zaštitu podataka u Belgiji, Estoniji, Francuskoj, Gruziji, Irskoj, Italiji, Mađarskoj, Monaku, Švicarskoj i Ujedinjenoj Kraljevini za korisne povratne informacije o nacrtu priručnika. Također želimo zahvaliti odjelu za zaštitu podataka Europske komisije te njezinu odjelu za međunarodne prijenose i zaštitu podataka. Zahvaljujemo Sudu Europske unije na podršci u vidu dokumentacije pružene tijekom pripreme ovog priručnika.

Zaključno, želimo izraziti zahvalnost Agenciji za zaštitu osobnih podataka na podršci prilikom revizije hrvatske verzije ovog priručnika.

Christos Giakoumopoulos

Glavni direktor Odjela
za ljudska prava i vladavinu
prava Vijeće Europe

Giovanni Buttarelli

Europski nadzornik
za zaštitu podataka

Michael O’Flaherty

Direktor Agencije
Europske unije
za temeljna prava

Sadržaj

PREDGOVOR	3
KRATICE I AKRONIMI	11
KAKO SE KORISTITI OVIM PRIRUČNIKOM	13
1 KONTEKST I POZADINA EUROPSKOG ZAKONODAVSTVA O ZAŠTITI	
PODATAKA	17
1.1. Pravo na zaštitu osobnih podataka	19
Ključne točke	19
1.1.1. Pravo na poštovanje privatnog života i pravo na zaštitu osobnih podataka: kratak uvod	20
1.1.2. Međunarodni pravni okvir: Ujedinjeni narodi	23
1.1.3. Europska konvencija o ljudskim pravima	24
1.1.4. Konvencija br. 108 Vijeća Europe	26
1.1.5. Zakonodavstvo Europske unije o zaštiti podataka	29
1.2. Ograničenja prava na zaštitu osobnih podataka	37
Ključne točke	37
1.2.1. Zahtjevi iz Europske konvencije o ljudskim pravima (EKLJP) koje je potrebno zadovoljiti kako bi miješanje bilo opravdano	39
1.2.2. Uvjeti za zakonita ograničenja u skladu s Poveljom Europske unije o temeljnim pravima	44
1.3. Odnos s drugim pravima i legitimnim interesima	54
Ključne točke	54
1.3.1. Sloboda izražavanja	55
1.3.2. Poslovna tajna	70
1.3.3. Sloboda vjeroispovijedi i uvjerenja	73
1.3.4. Sloboda umjetnosti i znanosti	75
1.3.5. Zaštita intelektualnog vlasništva	76
1.3.6. Zaštita podataka i gospodarski interesi	79
2 TERMINOLOGIJA POVEZANA SA ZAŠTITOM PODATAKA	83
2.1. Osobni podaci	85
Ključne točke	85
2.1.1. Glavni aspekti koncepta osobnih podataka	86
2.1.2. Posebne kategorije osobnih podataka	98

2.2.	Obrada podataka	100
	Ključne točke	100
2.2.1.	Koncept obrade podataka	100
2.2.2.	Automatizirana obrada podataka	101
2.2.3.	Neautomatizirana obrada podataka	103
2.3.	Korisnici osobnih podataka	104
	Ključne točke	104
2.3.1.	Voditelji obrade i izvršitelji obrade	104
2.3.2.	Primatelji i treće strane	113
2.4.	Privola	114
	Ključne točke	114
3	GLAVNA NAČELA EUROPSKOG ZAKONODAVSTVA O ZAŠTITI PODATAKA	117
3.1.	Načela zakonitosti, poštenosti i transparentnosti obrade	119
	Ključne točke	119
3.1.1.	Zakonitost obrade podataka	120
3.1.2.	Poštenost obrade podataka	120
3.1.3.	Transparentnost obrade podataka	122
3.2.	Načelo ograničenja svrhe	124
	Ključne točke	124
3.3.	Načelo smanjenja količine podataka	127
	Ključne točke	127
3.4.	Načelo točnosti podataka	129
	Ključne točke	129
3.5.	Načelo ograničenja pohrane	131
	Ključne točke	131
3.6.	Načelo sigurnosti podataka	133
	Ključne točke	133
3.7.	Načelo odgovornosti	136
	Ključne točke	136
4	ODREDBE EUROPSKOG ZAKONODAVSTVA O ZAŠTITI PODATAKA	141
4.1.	Propisi o zakonitoj obradi	144
	Ključne točke	144
4.1.1.	Zakonska osnova obrade podataka	144
4.1.2.	Obrada posebnih kategorija podataka (osjetljivih podataka)	161

4.2.	Pravila sigurnosti obrade	167
	Ključne točke	167
4.2.1.	Elementi sigurnosti podataka	167
4.2.2.	Povjerljivost	171
4.2.3.	Obavješćivanje u slučaju povrede osobnih podataka	173
4.3.	Propisi o odgovornosti i promicanju usklađenosti	176
	Ključne točke	176
4.3.1.	Službenici za zaštitu podataka	177
4.3.2.	Evidencija aktivnosti obrade	180
4.3.3.	Procjena učinka zaštite podataka i prethodno savjetovanje	181
4.3.4.	Kodeksi ponašanja	183
4.3.5.	Certificiranje	185
4.4.	Tehnička i integrirana zaštita podataka	185
5	NEOVISNI NADZOR	189
	Ključne točke	190
5.1.	Neovisnost	193
5.2.	Nadležnost i ovlasti	196
5.3.	Suradnja	199
5.4.	Europski odbor za zaštitu podataka	201
5.5.	Mehanizam konzistentnosti iz Opće uredbe o zaštiti podataka	203
6	PRAVA ISPITANIKA I NJIHOVA PROVEDBA	205
6.1.	Prava ispitanika	209
	Ključne točke	209
6.1.1.	Pravo na informacije	210
6.1.2.	Pravo na ispravak	222
6.1.3.	Pravo na brisanje („pravo na zaborav“)	224
6.1.4.	Pravo na ograničenje obrade	229
6.1.5.	Pravo na prenosivost podataka	230
6.1.6.	Pravo na prigovor	232
6.1.7.	Automatizirano pojedinačno donošenje odluka, uključujući izradu profila	236
6.2.	Pravni lijekovi, odgovornost, kazne i naknada	239
	Ključne točke	239
6.2.1.	Pravo na podnošenje pritužbe nadzornom tijelu	240
6.2.2.	Pravo na učinkovit pravni lijek	241
6.2.3.	Odgovornost i pravo na naknadu štete	248
6.2.4.	Sankcije	250

7	MEĐUNARODNI PRIJENOS PODATAKA I PROTOK OSOBNIH PODATAKA	253
7.1.	Priroda prijenosa osobnih podataka	255
	Ključne točke	255
7.2.	Slobodno kretanje/protok osobnih podataka među državama članicama ili ugovornim strankama	256
	Ključne točke	256
7.3.	Prijenosi osobnih podataka trećim zemljama/zemljama koje nisu stranke ili međunarodnim organizacijama	257
	Ključne točke	257
	7.3.1. Prijenosi na temelju odluke o primjerenosti	258
	7.3.2. Prijenosi koji podliježu odgovarajućim zaštitnim mjerama	263
	7.3.3. Odstupanja za posebne situacije	268
	7.3.4. Prijenosi koji se temelje na međunarodnim sporazumima	270
8	ZAŠTITA PODATAKA U KONTEKSTU POLICIJE I KAZNENOG PRAVOSUĐA	277
8.1.	Pravo Vijeća Europe u području zaštite podataka, nacionalne sigurnosti, policije i kaznenog pravosuđa	279
	Ključne točke	279
	8.1.1. Preporuka o policiji	281
	8.1.2. Budimpeštanska konvencija o kibernetičkom kriminalu	286
8.2.	Pravo Unije o zaštiti podataka u području policije i kaznenog pravosuđa	287
	Ključne točke	287
	8.2.1. Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa	288
8.3.	Ostali specifični pravni instrumenti za zaštitu podataka u slučajevima izvršavanja zakonodavstva	297
	8.3.1. Zaštita podataka u pravosudnim tijelima i agencijama za izvršavanje zakonodavstva EU-a	306
	8.3.2. Zaštita podataka u zajedničkim informacijskim sustavima na razini Europske unije	314
9	POSEBNE VRSTE PODATAKA I S NJIMA POVEZANI PROPISI O ZAŠTITI PODATAKA	331
9.1.	Elektroničke komunikacije	332
	Ključne točke	332
9.2.	Podaci o zaposlenju	336
	Ključne točke	336
9.3.	Zdravstveni podaci	341
	Ključna točka	341

9.4. Obrada podataka u istraživačke i statističke svrhe	345
Ključne točke	345
9.5. Financijski podaci	349
Ključne točke	349
10 SUVREMENI IZAZOVI U PODRUČJU ZAŠTITE OSOBNIH PODATAKA	353
10.1. Veliki podaci, algoritmi i umjetna inteligencija	355
Ključne točke	355
10.1.1. Definicije velikih podataka, algoritama i umjetne inteligencije	356
10.1.2. Odvagivanje koristi i rizika velikih podataka	359
10.1.3. Problemi povezani sa zaštitom podataka	361
10.2. Tehnologije Web 2.0 i 3.0: društvene mreže i internet stvari	367
Ključne točke	367
10.2.1. Definiranje tehnologija Web 2.0 i 3.0	367
10.2.2. Odvagivanje koristi i rizika	369
10.2.3. Problemi povezani sa zaštitom podataka	371
DODATNA LITERATURA	377
SUDSKA PRAKSA	385
Odabrana sudska praksa Europskog suda za ljudska prava	385
Odabrana sudska praksa Suda Europske unije	390
KAZALO	395

Kratice i akronimi

BCR	Obvezujuće korporativno pravilo
C-SIS	Središnji schengenski informacijski sustav
CCTV	Televizija zatvorenog kruga
CETS	Zbirka ugovora Vijeća Europe
CIS	Carinski informacijski sustav
CRM	Upravljanje odnosima s kupcima
DPA	Nadležno tijelo za zaštitu podataka
DPOSZP	Službenik za zaštitu podataka
EAW	Europski uhidbeni nalog
EDPS	Europski nadzornik za zaštitu podataka
EFSA	Europska agencija za sigurnost hrane
EFTA	Europsko udruženje slobodne trgovine
EGP	Europski gospodarski prostor
EKLJP	Europska konvencija o ljudskim pravima
ENISA	Agencija Europske unije za kibersigurnost
ENU	Europolova nacionalna jedinica
EOZP	Europski odbor za zaštitu podataka
EPPO	Ured europskog javnog tužitelja
ESLJP	Europski sud za ljudska prava
ESMA	Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala
eTEN	Transeuropske telekomunikacijske mreže
EU	Europska unija
eu-LISA	Agencija Europske unije za operativno upravljanje opsežnim informacijskim sustavima
EuroPriSe	Europski pečat za zaštitu podataka
EZ	Europska zajednica
FRA	Agencija Europske unije za temeljna prava
GPS	Globalni sustav pozicioniranja
IKCT	Informacijske i komunikacijske tehnologije
ISP	Pružatelj internetskih usluga

JSB	Zajedničko nadzorno tijelo
Konvencija br. 108	Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Vijeće Europe). Protokol o izmjeni (CETS br. 223) Konvencije br. 108 („modernizirana Konvencija br. 108“) donio je Odbor ministara Vijeća Europe prilikom 128. zasjedanja, održanog u Helsingøru u Danskoj (od 17. do 18. svibnja 2018.). Upućivanja na „moderniziranu Konvenciju br. 108“ odnose se na Konvenciju izmijenjenu Protokolom CETS br. 223.
MPGPP	Međunarodni pakt o građanskim i političkim pravima
N-SIS	Nacionalni schengenski informacijski sustav
NVO	Nevladina organizacija
ODLJP	Opća deklaracija o ljudskim pravima
OECD	Organizacija za ekonomsku suradnju i razvoj
OUZP	Opća uredba o zaštiti podataka
PIN	Osobni identifikacijski broj
PNR	Evidencija imena putnika
Povelja	Povelja Europske unije o temeljnim pravima
SCG	Koordinacijska skupina za nadzor
SEPA	Jedinstveno područje plaćanja u eurima
SEU	Sud Europske unije (prije prosinca 2009. poznat kao Europski sud, ECJ)
SIS	Schengenski informacijski sustav
SL	Službeni list
SWIFT	Društvo za svjetsku međubankovnu financijsku telekomunikaciju
UEU	Ugovor o Europskoj uniji
UFEU	Ugovor o funkcioniranju Europske unije
UN	Ujedinjeni narodi
VIS	Vizni informacijski sustav

Kako se koristiti ovim priručnikom

Ovaj priručnik pruža pregled pravnih standarda u vezi sa zaštitom podataka koje su utvrdili Europska unija (EU) i Vijeće Europe. Osmišljen je kao pomoć stručnjacima koji nisu specijalizirani u području zaštite podataka, uključujući odvjetnike, suce i druge pravne djelatnike, kao i zaposlenike drugih tijela kao što su nevladine organizacije (NVO) koji se mogu susresti s pravnim pitanjima povezanim sa zaštitom podataka.

Priručnik služi kao prva referentna točka za relevantno pravo Unije i Europsku konvenciju o ljudskim pravima (EKLJP), kao i za Konvenciju Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108) te druge instrumente Vijeća Europe.

Svako poglavlje započinje tablicom u kojoj su navedeni propisi povezani s temama iz pripadajućeg poglavlja. Tablice obuhvaćaju i pravo Vijeća Europe i pravo Unije te sadržavaju odabranu sudsku praksu Europskog suda za ljudska prava (ESLJP) i Suda Europske unije (SEU). Zatim se relevantni zakoni tih dvaju europskih sustava predstavljaju jedan za drugim prema primjenjivosti na svaku od tema. Tako čitatelji mogu saznati po čemu su ta dva pravna sustava slična, a po čemu se razlikuju. To bi čitateljima trebalo pomoći i u pronalaženju ključnih informacija koje se odnose na njihove slučajeve, osobito ako podliježu samo pravu Vijeća Europe. U određenim poglavljima, u kojima je to korisno za sažet prikaz sadržaja, redoslijed tema u tablicama može se donekle razlikovati od teksta samog poglavlja. U priručniku se također pruža kratak pregled okvira Ujedinjenih naroda.

Pravnici u državama koje nisu članice Unije, ali su članice Vijeća Europe te su ugovorne stranke Europske konvencije o ljudskim pravima i Konvencije br. 108, mogu pogledati informacije koje se odnose na njihove države izravno u odjeljcima koji se odnose na Vijeće Europe. Pravnici u državama koje nisu članice Unije moraju imati na umu i da se od donošenja Opće uredbe Europske unije o zaštiti podataka propisi EU-a o zaštiti podataka primjenjuju na organizacije i druge subjekte koji nemaju sjedište u EU-u ako obrađuju osobne podatke ispitanika u Uniji, pružaju im proizvode i usluge ili prate njihovo ponašanje.

Pravnici u državama članicama Unije morat će pogledati oba odjeljka jer su za te države obvezujuća oba pravna poretka. Vrijedi napomenuti da su reforme i modernizacija propisa o zaštiti podataka u Europi, pokrenute u okviru Vijeća Europe

(modernizirana Konvencija br. 108 izmijenjena Protokolom CETS br. 223) i u okviru EU-a (donošenje Opće uredbe o zaštiti podataka i Direktive (EU) 2016/680), uspo-redno provedene. Donositelji propisa u obama pravnim sustavima poduzeli su sve mjere kako bi osigurali dosljednost i usklađenost tih dvaju pravnih okvira. Reforma je stoga postignuta veća usklađenost zakonodavstva o zaštiti podataka Vijeća Europe i EU-a. Za osobe koje trebaju detaljnije informacije o određenoj temi predviđen je popis detaljnijih materijala u odjeljku pod nazivom „Dodatna literatura”. Informacije o odredbama Konvencije br. 108 i njezina dodatnog Protokola iz 2001., koje se primjenjuju do stupanja na snagu Protokola o izmjeni, dostupne su u izdanju priručnika iz 2014.

Pravo Vijeća Europe predstavljeno je kratkim upućivanjima na odabrane predmete ESLJP-a. Oni su odabrani iz velikog broja presuda i odluka tog suda u predmetima koji se odnose na zaštitu podataka.

Relevantno pravo EU-a obuhvaća donesene zakonodavne mjere, relevantne odredbe ugovorâ i Povelju Europske unije o temeljnim pravima, kako su protumačeni u sudskoj praksi SEU-a. Usto, priručnik donosi mišljenja i smjernice koje je donijela Radna skupina iz članka 29., savjetodavno tijelo koje je na temelju Direktive o zaštiti podataka dobilo zadatak pružanja stručnih savjeta državama članicama EU-a, a koje je od 25. svibnja 2018. zamijenio Europski odbor za zaštitu podataka (EOZP). Mišljenja Europskog nadzornika za zaštitu podataka također pružaju značajan uvid u tumačenje prava Unije, pa su stoga uvrštena u ovaj priručnik.

Predmetima opisanim ili citiranim u ovom priručniku daju se primjeri iz važnog skupa sudske prakse ESLJP-a i SEU-a. Smjernice na kraju priručnika služe kao pomoć čitateljima u pretraživanju sudske prakse na internetu. Prikazana sudska praksa SEU-a odnosi se na prijašnju Direktivu o zaštiti podataka. Međutim, tumačenja SEU-a i dalje su primjenjiva na pripadajuća prava i obveze utvrđene Općom uredbom o zaštiti podataka.

Nadalje, u tekstnim okvirima s plavom pozadinom prikazane su praktične ilustracije s hipotetskim scenarijima. Njima se dodatno objašnjava primjena europskih propisa o zaštiti podataka u praksi, osobito u slučajevima nepostojanja relevantne sudske prakse ESLJP-a ili SEU-a. U ostalim tekstnim okvirima, koji imaju sivu pozadinu, navode se primjeri preuzeti iz izvora koji ne pripadaju sudskoj praksi ESLJP-a i SEU-a, kao što su zakonodavstvo i mišljenja Radne skupine iz članka 29.

U uvodnom dijelu priručnika ukratko je opisana uloga dvaju pravnih sustava uspostavljenih Europskom konvencijom o ljudskim pravima i pravom Unije (poglavlje 1.). Poglavlja od 2. do 10. obuhvaćaju sljedeće teme:

- terminologija povezana sa zaštitom podataka,
- glavna načela europskog zakonodavstva o zaštiti podataka,
- propisi europskog zakonodavstva o zaštiti podataka,
- neovisni nadzor,
- prava ispitanika i njihova provedba,
- prekogranični prijenosi osobnih podataka,
- zaštita podataka u kontekstu policije i kaznenog pravosuđa,
- ostali europski propisi o zaštiti podataka u određenim područjima,
- suvremeni izazovi u području zaštite osobnih podataka.

1

Kontekst i pozadina europskog zakonodavstva o zaštiti podataka



EU	Obuhvaćena pitanja	Vijeće Europe
Pravo na zaštitu podataka		
Ugovor o funkcioniranju Europske unije, članak 16.		EKLJP, članak 8. (pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja)
Povelja Europske unije o temeljnim pravima (Povelja), članak 8. (pravo na zaštitu osobnih podataka)		Modernizirana Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (modernizirana Konvencija br. 108)
Direktiva 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Direktiva o zaštiti podataka), SL 1995 L 281 (na snazi do svibnja 2018.)		
Okvirna odluka Vijeća 2008/977/PUP o zaštiti osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima, SL 2008 L 350 (na snazi do svibnja 2018.)		
Uredba (EU) 2016/679 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL 2016 L 119		
Direktiva (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (zaštita podataka za policiju i tijela kaznenog prava), SL 2016 L 119		

EU	Obuhvaćena pitanja	Vijeće Europe
Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL 2002 L 201 Uredba (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (Uredba o zaštiti podataka u institucijama Europske unije), SL 2001 L 8		
Ograničenje prava na zaštitu osobnih podataka		
Povelja, članak 52. stavak 1. Opća uredba o zaštiti podataka, članak 23. SEU, spojeni predmeti C-92/09 i C-93/09, <i>Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen</i> [VV], 2010.		EKLJP, članak 8. stavak 2. Modernizirana Konvencija br. 108, članak 11. ESLJP, <i>S. i Marper protiv Ujedinjene Kraljevine</i> [VV], br. 30562/04 i 30566/04, 2008.
Uravnoteživanje prava		
SEU, spojeni predmeti C-92/09 i C-93/09, <i>Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen</i> [VV], 2010.	Općenito	
SEU, C-73/07, <i>Tietosuoja-vaikuttettut protiv Satakunnan Markkinapörssi Oy i Satamedia Oy</i> [VV], 2008. SEU, C-131/12, <i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González</i> [VV], 2014.	Sloboda izražavanja	ESLJP, <i>Axel Springer AG protiv Njemačke</i> [VV], br. 39954/08, 2012. ESLJP, <i>Mosley protiv Ujedinjene Kraljevine</i>, br. 48009/08, 2011. ESLJP, <i>Bohlen protiv Njemačke</i>, br. 53495/09, 2015.
SEU, C-28/08 P, <i>Europska komisija protiv The Bavarian Lager Co. Ltd</i> [VV], 2010. SEU, C-615/13 P, <i>ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA) i Europske komisije</i>, 2015.	Pristup dokumentima	ESLJP, <i>Magyar Helsinki Bizottság protiv Mađarske</i> [VV], br. 18030/11, 2016.
Opća uredba o zaštiti podataka, članak 90.	Poslovna tajna	ESLJP, <i>Pruteanu protiv Rumunjske</i>, br. 30181/05, 2015.
Opća uredba o zaštiti podataka, članak 91.	Sloboda vjeroispovijedi ili uvjerenja	

EU	Obuhvaćena pitanja	Vijeće Europe
	Sloboda umjetnosti i znanosti	ESLJP, <i>Vereinigung bildender Künstler protiv Austrije</i> , br. 68354/01, 2007.
SEU, C-275/06, <i>Productores de Música de España (Promusicae) protiv Telefónica de España SAU</i> [VV], 2008.	Zaštita vlasništva	
SEU, C-131/12, <i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González</i> [VV], 2014. SEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija</i> , 2017.	Ekonomska prava	

1.1. Pravo na zaštitu osobnih podataka

Ključne točke

- Prema članku 8. Europske konvencije o ljudskim pravima, pravo na zaštitu pojedinca u pogledu obrade osobnih podataka dio je prava na poštovanje privatnog i obiteljskog života, doma i dopisivanja.
- Konvencija br. 108 Vijeća Europe prvi je i trenutačno jedini međunarodni pravno obvezujući instrument koji se bavi zaštitom podataka. Konvencija je modernizirana i dopunjena donošenjem Protokola o izmjeni CETS br. 223.
- Prema pravu EU-a, zaštita podataka priznata je kao zasebno temeljno pravo. To je potvrđeno člankom 16. Ugovora o funkcioniranju Europske unije i člankom 8. Povelje EU-a o temeljnim pravima.
- Prema pravu EU-a, zaštita podataka prvi je put regulirana 1995. Direktivom o zaštiti podataka.
- Uzimajući u obzir brz tehnološki razvoj, EU je 2016. donio nove zakone kako bi propise o zaštiti podataka prilagodio digitalnom dobu. Opća uredba o zaštiti podataka stupila je na snagu u svibnju 2018. i njome je Direktiva o zaštiti podataka stavljena izvan snage.
- Uz Opću uredbu o zaštiti podataka, EU je donio zakone o obradi osobnih podataka koju provode državna tijela u svrhu izvršavanja zakonodavstva. Direktivom (EU) 2016/680 utvrđuju se pravila i načela zaštite podataka kojima se uređuje obrada osobnih podataka u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija.

1.1.1. Pravo na poštovanje privatnog života i pravo na zaštitu osobnih podataka: kratak uvod

Iako su usko povezana, pravo na poštovanje privatnog života i pravo na zaštitu osobnih podataka zasebna su prava. Pravo na privatnost, koje se u europskom zakonodavstvu naziva pravom na poštovanje privatnog života, uvedeno je u međunarodno zakonodavstvo o ljudskim pravima Općom deklaracijom o ljudskim pravima (ODLJP) iz 1948. kao jedno od temeljnih zaštićenih ljudskih prava. Ubrzo nakon donošenja ODLJP-a Europa je potvrdila to pravo Europskom konvencijom o ljudskim pravima (EKLJP), sporazumom sastavljenim 1950. koji je pravno obvezujući za njegove ugovorne stranke. EKLJP-om se određuje da svaka osoba ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i dopisivanja. Javnim tijelima zabranjuje se miješanje u to pravo, osim u slučajevima u kojima je to u skladu sa zakonom, kada se time nastoji ostvariti važan i legitiman javni interes ili je to nužno u demokratskom društvu.

ODLJP i EKLJP doneseni su mnogo prije razvoja računala i interneta te pojave informacijskog društva. To je donijelo znatne prednosti pojedincima i društvu te poboljšalo kvalitetu života, učinkovitost i produktivnost. S druge strane, pojavili su se i novi rizici za pravo na poštovanje privatnog života. Kao odgovor na potrebu za posebnim propisima kojima se uređuje prikupljanje i upotreba osobnih podataka, uveden je nov koncept privatnosti, koji se u nekim pravnim sustavima naziva „informacijska privatnost“, a u nekima „pravo na informacijsko samoodređenje“¹. Taj je koncept doveo do razvoja posebnih zakonskih propisa kojima se osigurava zaštita osobnih podataka.

Zaštita podataka u Europi započela je 1970-ih kada su u nekim državama doneseni propisi vezani za regulaciju obrade osobnih podataka koju provode javna tijela i velika društva². Nakon toga uspostavljeni su instrumenti za zaštitu podataka na

1 Savezni ustavni sud Njemačke potvrdio je pravo na informacijsko samoodređenje presudom u predmetu *Volkszählungsurteil* iz 1983., BverfGE Bd. 65, S. 1ff. Sud je zaključio da informacijsko samoodređenje proizlazi iz temeljnog prava na poštovanje osobnosti, koje je zaštićeno njemačkim Ustavom. ESLJP je presudom iz 2017. potvrdio da se člankom 8. EKLJP-a „jamči pravo na oblik informacijskog samoodređenja“. Vidjeti ESLJP, *Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske* [VV], br. 931/13, 27. lipnja 2017., t. 137.

2 Njemačka savezna država Hessen donijela je 1970. prvi zakon o zaštiti podataka, koji se primjenjivao samo u toj državi. Švedska je 1973. donijela prvi nacionalni zakon o zaštiti podataka u svijetu. Do kraja 1980-ih nekoliko je europskih država (Francuska, Njemačka, Nizozemska i Ujedinjena Kraljevina) također donijelo zakone o zaštiti podataka.

razini Europe³ te se s vremenom zaštita podataka razvila u posebnu vrijednost koja nije obuhvaćena pravom na poštovanje privatnog života. U pravnom poretku EU-a zaštita podataka priznata je kao temeljno pravo odvojeno od temeljnog prava na poštovanje privatnog života. Zbog takva se razdvajanja postavlja pitanje odnosa i razlika između tih prava.

Pravo na poštovanje privatnog života i pravo na zaštitu osobnih podataka usko su povezani. Obima se nastoje zaštititi slične vrijednosti, odnosno autonomija i ljudsko dostojanstvo pojedinaca, osiguravanjem osobne sfere u kojoj mogu slobodno razvijati svoje osobnosti, razmišljati i oblikovati vlastita mišljenja. Ona su stoga nužan preduvjet za ostvarivanje temeljnih sloboda, kao što su sloboda izražavanja, sloboda mirnog okupljanja i udruživanja te sloboda vjeroispovijedi.

Ta dva prava razlikuju se prema formulaciji i području primjene. Pravo na poštovanje privatnog života uključuje opću zabranu miješanja, osim u određenim slučajevima postojanja javnog interesa koji bi mogao opravdati takvo miješanje. Zaštita osobnih podataka smatra se suvremenim i aktivnim pravom⁴ kojim se uspostavlja sustav provjera i kontrole kako bi se pojedinci zaštitili prilikom svake obrade njihovih podataka. Obrada mora biti u skladu s osnovnim elementima zaštite osobnih podataka, prvenstveno neovisnim nadzorom i poštovanjem prava ispitanika⁵.

Člankom 8. Povelje EU-a o temeljnim pravima (Povelja) potvrđuje se pravo na zaštitu osobnih podataka te se iznose temeljne vrijednosti povezane s tim pravom. Njime se utvrđuje da obrada osobnih podataka mora biti poštena, da se mora provoditi u utvrđene svrhe i temeljiti se na privoli osobe o kojoj je riječ ili legitimnoj osnovi utvrđenoj zakonom. Pojedinci moraju imati pravo na pristup svojim osobnim podacima i pravo na njihovo ispravljanje, a poštovanje tog prava mora podlijeagati nadzoru neovisnog tijela.

3 Konvencija Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108) donesena je 1981. EU je 1995. donio prvi sveobuhvatni instrument zaštite podataka: Direktivu 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka.

4 Nezavisna odvjetnica Sharpston navela je da predmet obuhvaća dva zasebna prava: „klasično“ pravo na zaštitu privatnosti i „suvremenije“ pravo na zaštitu podataka. Vidjeti SEU, spojeni predmeti C-92/09 i C-93/02, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen, Mišljenje nezavisnog odvjetnika Sharpston*, 17. lipnja 2010., t. 71.

5 Hustinx, P., Govori i članci EDPS-a, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, srpanj 2013.

Pravo na zaštitu osobnih podataka primjenjuje se prilikom svake obrade osobnih podataka, te je stoga šire od prava na poštovanje privatnog života. Svaki postupak obrade osobnih podataka podliježe odgovarajućoj zaštiti. Zaštita podataka obuhvaća razne vrste osobnih podataka i obrade podataka, neovisno o njihovu odnosu i utjecaju na privatnost. Obradom osobnih podataka također se može kršiti pravo na privatni život, kao što je vidljivo u primjerima u nastavku. Međutim, nije potrebno dokazati kršenje prava na privatni život kako bi se primijenila pravila zaštite podataka.

Pravo na privatnost odnosi se na situacije u kojima je ugrožen privatni interes ili „privatni život” pojedinca. Kao što će biti pokazano u ovom priručniku, koncept „privatnog života” u sudskoj se praksi široko tumači, tako da obuhvaća intimne situacije, osjetljive ili povjerljive informacije, informacije koje bi mogle dovesti do predrasuda protiv neke osobe u javnosti, a obuhvaća čak i aspekte nečijeg profesionalnog života i ponašanja u javnosti. Međutim, procjena postojanja umiješanosti u „privatni život” ovisi o kontekstu i okolnostima svakog pojedinog slučaja.

S druge strane, svaka radnja koja uključuje obradu osobnih podataka može biti obuhvaćena područjem primjene propisa o zaštiti podataka i uvjetovati provođenje prava na zaštitu osobnih podataka. Na primjer, ako poslodavac bilježi informacije o imenima i naknadama zaposlenika, samo bilježenje tih informacija ne može se smatrati miješanjem u privatni život. To bi se, međutim, moglo smatrati miješanjem ako bi poslodavac te osobne podatke zaposlenika prenosio trećim stranama. Poslodavci se u svakom slučaju moraju pridržavati propisa o zaštiti podataka jer bilježenje podataka o zaposlenicima predstavlja obradu podataka.

Primjer: U predmetu *Digital Rights Ireland*⁶ SEU je trebao donijeti odluku o valjanosti Direktive 2006/24/EZ u kontekstu temeljnih prava na zaštitu osobnih podataka i poštovanje privatnog života, koja su potvrđena Poveljom EU-a o temeljnim pravima. Direktivom se pružateljima javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža nalogalo zadržavanje telekomunikacijskih podataka građana najviše dvije godine kako bi se osiguralo da podaci budu dostupni u svrhe sprečavanja, istrage i progona teških kaznenih djela. Ta se mjera odnosila samo na metapodatke, podatke o lokaciji i podatke nužne za identifikaciju pretplatnika ili korisnika. Nije se primjenjivala na sadržaj elektroničkih komunikacija.

6 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VW], 8. travnja 2014.

SEU je zaključio da Direktiva predstavlja miješanje u temeljno pravo na zaštitu osobnih podataka „s obzirom na to da predviđa obradu osobnih podataka”⁷. Također je zaključio da se Direktiva upliće u pravo na poštovanje privatnog života⁸. Uzeti zajedno, osobni podaci zadržani sukladno Direktivi, kojima mogu pristupiti nadležna tijela, mogu omogućiti „donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podaci zadržani, kao što su svakodnevne navike, mjesta trajnih ili privremenih boravaka, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posjećivale”⁹. Miješanje u spomenuta dva prava bilo je široko i osobito teško.

SEU je Direktivu 2006/24/EZ proglasio nevaljanom, zaključivši da je, iako se njome nastojao ostvariti legitiman cilj, miješanje u prava na zaštitu osobnih podataka i privatni život bilo teško i nije bilo ograničeno na ono što je strogo nužno.

1.1.2. Međunarodni pravni okvir: Ujedinjeni narodi

U okviru Ujedinjenih naroda zaštita osobnih podataka nije prepoznata kao temeljno pravo, iako je pravo na privatnost dugo ustaljeno temeljno pravo u međunarodnom pravnom poretku. Članak 12. Opće deklaracije o ljudskim pravima (ODLJP) o poštovanju privatnog i obiteljskog života¹⁰ prvi je slučaj u kojemu je međunarodnim instrumentom utvrđeno pravo pojedinca na zaštitu njegove privatne sfere od miješanja drugih, osobito države. Iako je riječ o neobvezujućoj deklaraciji, ODLJP ima značajan status temeljnog instrumenta međunarodnog prava o ljudskim pravima te je utjecao na razvoj drugih instrumenata ljudskih prava u Europi. Međunarodni pakt o građanskim i političkim pravima (MPGPP) stupio je na snagu 1976. U njemu se navodi da nitko ne smije biti podvrgnut samovoljnom ili nezakonitom miješanju u njegov privatni život, obitelj ili dopisivanje, ni nezakonitim napadima na njegovu čast ili ugled. MPGPP je međunarodni sporazum kojim se njegovih 169 potpisnika obvezuje na poštovanje i jamčenje provedbe građanskih prava pojedinaca, uključujući privatnost.

⁷ *Ibid.*, t. 36.

⁸ *Ibid.*, t. od 32. do 35.

⁹ *Ibid.*, t. 27.

¹⁰ Ujedinjeni narodi (UN), *Opća Deklaracija o Ljudskim Pravima*, 10. prosinca 1948.

Nakon 2013. Ujedinjeni narodi donijeli su dvije rezolucije povezane s pitanjem privatnosti pod nazivom „pravo na privatnost u digitalnom dobu”¹¹ kao odgovor na razvoj novih tehnologija i razotkrivanje slučajeva masovnog nadzora u nekim državama (objava informacija Edwarda Snowdena). U njima je iznesena snažna osuda masovnog nadzora i istaknut učinak koji takav nadzor može imati na temeljna prava na privatnost i slobodu izražavanja, kao i na funkcioniranje dinamičnog, demokratskog društva. Iako rezolucije nisu pravno obvezujuće, potaknule su važnu međunarodnu političku raspravu na visokoj razini o privatnosti, novim tehnologijama i nadzoru. Također su dovele do imenovanja posebnog izvijestitelja UN-a za pitanja prava na privatnost, s ovlašću promicanja i zaštite tog prava. Posebni zadaci izvijestitelja uključuju prikupljanje informacija o nacionalnim praksama i iskustvima u vezi s privatnošću i izazovima koji proizlaze iz novih tehnologija, razmjenu i promicanje najboljih praksi te utvrđivanje mogućih prepreka.

Prijašnje su rezolucije bile usmjerene na negativne učinke masovnog nadzora i odgovornost vlada da ograniče ovlasti obavještajnih službi, dok se u novijim rezolucijama odražava ključna nova pojava u raspravi o privatnosti u Ujedinjenim narodima¹². U rezolucijama donesenima 2016. i 2017. potvrđuje se potreba za ograničenjem ovlasti obavještajnih agencija i osuđuje masovni nadzor. Međutim, u njima se također izričito navodi da „sve veća mogućnost poduzeća da prikupljaju, obrađuju i upotrebljavaju osobne podatke može predstavljati rizik za uživanje prava na privatnost u digitalnom dobu”. Stoga se uz odgovornost državnih tijela u rezolucijama ističe i odgovornost privatnog sektora da poštuje ljudska prava te se tvrtke potiču na obavještavanje korisnika o prikupljanju, upotrebi, dijeljenju i zadržavanju osobnih podataka i na donošenje transparentnih pravila o obradi podataka.

1.1.3. Europska konvencija o ljudskim pravima

Vijeće Europe osnovano je nakon Drugog svjetskog rata kako bi približilo države Europe u nastojanjima za promicanjem vladavine prava, demokracije, ljudskih prava i društvenog razvoja. U tu je svrhu Vijeće 1950. donijelo [Europsku konvenciju o ljudskim pravima \(EKLJP\)](#), koja je stupila na snagu 1953.

11 Vidjeti UN, Opća skupština, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18. prosinca 2013.; i UN, Opća skupština, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/69/L.26/Rev. 1, New York, 19. studenoga 2014.

12 UN, Opća skupština, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/71/L.39/Rev. 1, New York, 16. studenoga 2016.; UN, Vijeće za ljudska prava, *The right to privacy in the digital age*, A/HRC/34/L.7/Rev. 1, 23. ožujka 2017.

Ugovorne stranke Konvencije imaju međunarodnu obvezu njezina poštovanja. Sve države članice Vijeća Europe ugradile su ili provele EKLJP u svojim nacionalnim zakonodavstvima, što ih obvezuje na poštovanje odredbi Konvencije. Ugovorne stranke moraju poštovati prava navedena u Konvenciji prilikom izvršavanja bilo kakve aktivnosti ili provođenja ovlasti. To uključuje aktivnosti poduzete radi nacionalne sigurnosti. Povijesne presude Europskog suda za ljudska prava (ESLJP) odnosile su se na državne aktivnosti u osjetljivim područjima zakonodavstva i prakse u vezi s nacionalnom sigurnošću¹³. Sud je bez oklijevanja potvrdio da aktivnosti nadzora predstavljaju miješanje u poštovanje privatnog života¹⁴.

Kako bi se osiguralo da ugovorne stranke poštuju svoje obveze preuzete EKLJP-om, u Strasbourgu, u Francuskoj, osnovan je 1959. godine Europski sud za ljudska prava (ESLJP). Taj sud osigurava da države poštuju obveze preuzete Konvencijom te razmatra žalbe pojedinaca, skupina pojedinaca, nevladinih organizacija ili pravnih osoba zbog navodnog kršenja Konvencije. ESLJP može razmatrati i međudržavne predmete koje neka država članica Vijeća Europe (ili više njih) podnese protiv druge države članice.

Vijeće Europe 2018. godine brojilo je 47 država članica, od kojih su 28 i države članice Europske unije. Tužitelj koji se obraća ESLJP-u ne mora biti državljanin ugovorne stranke, no navodna kršenja moraju se dogoditi na području pravne nadležnosti jedne od ugovornih stranaka.

Pravo na zaštitu osobnih podataka dio je prava zaštićenih člankom 8. EKLJP-a, kojim se jamči pravo na poštovanje privatnog i obiteljskog života, doma i dopisivanja te propisuju uvjeti u kojima su dopuštena ograničenja toga prava¹⁵.

ESLJP je razmatrao mnoge situacije povezane s pitanjima zaštite podataka. One uključuju presretanje komunikacije,¹⁶ razne oblike nadzora koje provode i privatni

13 Primjerice, vidjeti sljedeće: ESLJP, *Klass i drugi protiv Njemačke*, br. 5029/71, 6. rujna 1978.; ESLJP, *Rotaru protiv Rumunjske* [VV], br. 28341/95, 4. svibnja 2000. i ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. siječnja 2016.

14 *Ibid.*

15 Vijeće Europe, *European Convention on Human Rights*, CETS br. 005, 1950.

16 Primjerice, vidjeti sljedeće: ESLJP, *Malone protiv Ujedinjene Kraljevine*, br. 8691/79, 2. kolovoza 1984.; ESLJP, *Copland protiv Ujedinjene Kraljevine*, br. 62617/00, 3. travnja 2007., ili ESLJP, *Mustafa Sezgin Tanrıkulu protiv Turske*, br. 27473/06, 18. srpnja 2017.

i javni sektor¹⁷ i zaštitu od pohrane osobnih podataka koju obavljaju javna tijela¹⁸. Poštovanje privatnog života nije apsolutno pravo jer se ostvarivanjem prava na privatnost mogu ugroziti druga prava, kao što su sloboda izražavanja i pristupa informacijama, i obrnuto. Stoga ESLJP nastoji postići ravnotežu između različitih prava o kojima je riječ. Pojasnio je da se člankom 8. EKLP-a države obvezuju ne samo na suzdržavanje od svih radnji kojima bi mogle prekršiti to pravo iz Konvencije već i da ih se u određenim okolnostima pozitivno obvezuje na aktivno promicanje učinkovitog poštovanja privatnog i obiteljskog života¹⁹. Mnogi od tih slučajeva podrobno su opisani u odgovarajućim poglavljima.

1.1.4. Konvencija br. 108 Vijeća Europe

Od pojave informacijske tehnologije 1960-ih godina rasla je potreba za detaljnijim propisima kojima bi se zaštitili osobni podaci pojedinaca. Sredinom 70-ih godina Odbor ministara Vijeća Europe donio je više rezolucija o zaštiti osobnih podataka pozivajući se na članak 8. EKLP-a²⁰. [Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka \(Konvencija br. 108\)](#)²¹ otvorena je za potpisivanje 1981. Konvencija br. 108 bila je i ostala jedini pravno obvezujući međunarodni instrument u području zaštite podataka.

Konvencija br. 108 primjenjuje se na svaku obradu podataka u privatnom i u javnom sektoru, uključujući obradu u sudstvu i obradu koju obavljaju tijela zadužena za izvršavanje zakonodavstva. Konvencija štiti pojedince od zlouporaba prilikom obrade osobnih podataka i njome se istodobno nastoje regulirati prekogranični prijenosi osobnih podataka. U pogledu obrade osobnih podataka, načela iz Konvencije osobito se tiču pravednog i zakonitog prikupljanja i automatske obrade podataka u određene legitimne svrhe. To znači da se podaci ne smiju upotrebljavati u druge, neprikladne svrhe i da se ne smiju zadržavati dulje no što je potrebno. Ta se načela odnose i na

17 Primjerice, vidjeti sljedeće: ESLJP, *Klass i drugi protiv Njemačke*, br. 5029/71, 6. rujna 1978.; ESLJP, *Uzun protiv Njemačke*, br. 35623/05, 2. rujna 2010.

18 Primjerice, vidjeti sljedeće: ESLJP, *Roman Zakharov protiv Rusije* [VV], br. 47143/06, 4. prosinca 2015.; ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. siječnja 2016.

19 Primjerice, vidjeti sljedeće: ESLJP, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.; ESLJP, *K. U. protiv Finske*, br. 2872/02, 2. prosinca 2008.

20 Vijeće Europe, Odbor ministara (1973.), *Rezolucija (73) 22* o zaštiti privatnosti pojedinaca vis-à-vis elektroničkih banki podataka u privatnom sektoru, 26. rujna 1973.; Vijeće Europe, Odbor ministara (1974.), *Rezolucija (74) 29* o zaštiti privatnosti pojedinaca vis-à-vis elektroničkih banki podataka u javnom sektoru, 20. rujna 1974.

21 Vijeće Europe, Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, CETS br. 108, 1981.

kvalitetu podataka: oni u prvom redu moraju biti prikladni, relevantni, točni i ne smiju biti pretjerani (proporcionalnost).

Osim jamstava u pogledu obrade osobnih podataka i obveza sigurnosti podataka, Konvencijom se – u slučaju izostanka prikladnih pravnih mjera zaštite – zabranjuje obrada „osjetljivih” podataka, kao što su rasa, političko opredjeljenje, zdravlje, vjera, seksualni život ili kaznena evidencija pojedinca.

Njome se također štiti pravo pojedinca na informiranost o tome pohranjuju li se podaci o njemu te, ako je to nužno, pravo na ispravljanje takvih podataka. Ograničenja prava utvrđenih Konvencijom moguća su samo kada su posrijedi važniji interesi, kao što je sigurnost ili obrana države. Osim što se Konvencijom omogućuje slobodan prijenos osobnih podataka među njezinim ugovornim strankama, njome se također nameću određena ograničenja prijenosa u države čije pravno uređenje ne pruža jednaku razinu zaštite.

Vrijedi napomenuti da je Konvencija br. 108 obvezujuća za države koje su je ratificirale. Konvencija ne podliježe sudskom nadzoru ESLJP-a, no razmatra se u okviru sudske prakse ESLJP-a u kontekstu članka 8. EKLJP-a. Tijekom godina ESLJP je presuđivao da je zaštita osobnih podataka važan dio prava na poštovanje privatnog života (članak 8.) te se vodio načelima Konvencije br. 108 u odlučivanju o postojanju miješanja u to temeljno pravo²².

Kako bi nastavio razvijati opća načela i pravila iz Konvencije br. 108, Odbor ministara Vijeća Europe donio je nekoliko pravno neobvezujućih preporuka. Te su preporuke pridonijele razvoju zakonodavstva o zaštiti podataka u Europi. Primjerice, godinama je jedini instrument koji je pružao smjernice o uporabi osobnih podataka u policijskom sektoru u Europi bila Preporuka o policiji²³. Načela Preporuke – kao što su načini čuvanja baza podataka i potreba za provođenjem jasnih pravila o osobama kojima je dopušten pristup tim bazama – dodatno su razvijena i ugrađena u naknadno zakonodavstvo EU-a²⁴. Novije preporuke usmjerene su na rješavanje izazova digitalnog doba, primjerice u vezi s obradom podataka u kontekstu zapošljavanja (vidjeti poglavlje 9.).

22 Primjerice, vidjeti sljedeće: ESLJP, *Z protiv Finske*, br. 22009/93, 25. veljače 1997.

23 Vijeće Europe, Odbor ministara (1987.), Preporuka Rec(87)15 državama članicama o uporabi osobnih podataka u policijskom sektoru, Strasbourg, 17. rujna 1987.

24 Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23. studenoga 1995.

Sve su države članice EU-a ratificirale Konvenciju br. 108. Godine 1999. predložene su izmjene Konvencije br. 108 kako bi se omogućilo da EU postane ugovorna stranka, no nikada nisu stupile na snagu²⁵. Dodatni protokol uz Konvenciju br. 108 donesen je 2001. Njime su uvedene odredbe o prekograničnom prijenosu podataka u zemlje koje nisu ugovorne stranke Konvencije, tzv. trećim zemljama, te o obveznom uspostavljanju nacionalnih tijela nadležnih za zaštitu podataka²⁶.

Konvenciji br. 108 mogu pristupiti države koje nisu članice Vijeća Europe. Potencijal Konvencije kao univerzalnog standarda i njezin otvoren karakter služe kao temelj promicanja zaštite podataka na globalnoj razini. Do sada je 51 zemlja potpisala Konvenciju br. 108. Među njima su sve države članice Vijeća Europe (47 zemalja), Urugvaj, prva neeuropska zemlja koja je pristupila Konvenciji, u kolovozu 2013., te Mauricijus, Senegal i Tunis, koji su pristupili 2016. i 2017.

Konvencija je nedavno podvrgnuta postupku **modernizacije**. Javno savjetovanje provedeno 2011. potvrdilo je dva glavna cilja tog postupka: veću zaštitu privatnosti u digitalnom okruženju i jačanje mehanizma praćenja provedbe Konvencije. Postupak modernizacije bio je usmjeren na te ciljeve, a dovršen je donošenjem protokola o izmjeni Konvencije br. 108 (Protokol CETS br. 223). Postupak se provodio istodobno s drugim reformama međunarodnih instrumenata za zaštitu podataka te reformom propisa EU-a o zaštiti podataka pokrenutom 2012. Donositelji propisa na razini Vijeća Europe i EU-a poduzeli su sve mjere kako bi osigurali dosljednost i usklađenost tih dvaju pravnih okvira. Modernizacijom je očuvan opći i fleksibilan karakter Konvencije i potvrđen potencijal Konvencije kao univerzalnog pravnog instrumenta u području zaštite podataka. Njome se potvrđuju i stabiliziraju važna načela i pružaju nova prava pojedincima, a istodobno se povećavaju i osiguravaju odgovornosti tijela koja obrađuju osobne podatke. Primjerice, osobe čiji se osobni podaci obrađuju imaju pravo saznati razloge za takvu obradu podataka i imaju pravo na prigovor na obradu. Kako bi se suzbio porast profiliranja na mreži, Konvencijom se također utvrđuje pravo pojedinca da ne bude predmet odluka koje se temelje isključivo na automatiziranoj obradi, bez uzimanja u obzir njegova mišljenja. Učinkovita provedba propisa o zaštiti podataka koju obavljaju neovisna nadzorna tijela u zemljama ugovornim strankama smatra se ključnom za provedbu Konvencije u praksi. Zbog toga

25 Vijeće Europe, Izmjene Konvencije o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (ETS br. 108), koje je donio Odbor ministara u Strasbourgu, 15. lipnja 1999.

26 Vijeće Europe, Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, CETS br. 181, 2001. Modernizacijom Konvencije br. 108 ovaj se protokol prestao primjenjivati jer su njegove odredbe izmijenjene i ugrađene u moderniziranu Konvenciju br. 108.

se u moderniziranoj Konvenciji ističe potreba za davanjem učinkovitih ovlasti i funkcija nadzornim tijelima te za njihovom stvarnom neovisnosti u ostvarivanju njihove misije.

1.1.5. Zakonodavstvo Europske unije o zaštiti podataka

Pravo EU-a sastoji se od primarnog i sekundarnog prava. Ugovore, odnosno [Ugovor o Europskoj uniji \(UEU\)](#) i Ugovor o funkcioniranju Europske unije (UFEU), ratificirale su sve države članice EU-a i oni zajedno čine „primarno pravo Unije“. Uredbe, direktive i odluke EU-a donijele su institucije EU-a koje su za to ovlaštene ugovorima i one zajedno čine „sekundarno pravo EU-a“.

Zaštita podataka u primarnom pravu EU-a

U izvornim ugovorima Europskih zajednica nisu se spominjala ljudska prava ni njihova zaštita jer je Europska ekonomska zajednica prvotno bila zamišljena kao regionalna organizacija usmjerena na ekonomsku integraciju i uspostavljanje zajedničkog tržišta. Temeljno načelo na kojem počivaju osnivanje i razvoj Europskih zajednica, koje je jednako aktualno i danas, jest načelo dodjele. Prema tom načelu, EU djeluje isključivo unutar nadležnosti koje mu dodijele države članice, što je utvrđeno ugovorima o EU-u. Za razliku od Vijeća Europe, u ugovorima o EU-u ne utvrđuje se nikakva izričita nadležnost u pogledu temeljnih prava.

Međutim, budući da su se pred SEU-om iznosili predmeti o navodnim kršenjima ljudskih prava u području primjene prava EU-a, SEU je dao važno tumačenje ugovorâ. Kako bi zajamčio zaštitu pojedincima, ugradio je temeljna prava u takozvana opća načela europskog zakonodavstva. Prema Sudu Europske unije, ta opća načela odražavaju sadržaj zaštite ljudskih prava iz nacionalnih ustava i ugovora o ljudskim pravima, a osobito EKLJP-a. SEU je naveo da će osigurati usklađenost prava EU-a s tim načelima.

Uviđajući da njezine politike mogu utjecati na ljudska prava i nastojeći izgraditi „bliiskiji“ odnos sa svojim državljanima, Europska unija proglasila je 2000. Povelju Europske unije o temeljnim pravima (Povelja). Ona obuhvaća cijeli niz građanskih, političkih, ekonomskih i socijalnih prava europskih građana i sintetizira ustavne tradicije i međunarodne obveze zajedničke državama članicama. Prava opisana u Povelji

dijele se u šest kategorija: dostojanstvo, slobode, jednakost, solidarnost, prava građana i pravda.

Povelja je u početku bila samo politički dokument, no stupanjem na snagu Ugovora iz Lisabona 1. prosinca 2009. postala je pravno obvezujuća²⁷ kao primarno pravo EU-a (vidjeti članak 6. stavak 1. Ugovora o Europskoj uniji)²⁸. Odredbe Povelje namijenjene su institucijama i tijelima EU-a te su oni pri izvršavanju svojih dužnosti obvezni poštovati prava navedena u njoj. Odredbe Povelje obvezujuće su za države članice i prilikom provedbe prava EU-a.

Poveljom se ne samo jamči poštovanje privatnog i obiteljskog života (članak 7.) nego se i utvrđuje pravo na zaštitu osobnih podataka (članak 8.). Poveljom se razina te zaštite izričito podiže na razinu zaštite temeljnih prava u okviru prava EU-a. Institucije i tijela EU-a moraju jamčiti i poštovati to pravo, kao i države članice pri provedbi prava EU-a (članak 51. Povelje). Formuliran nekoliko godina nakon Direktive o zaštiti podataka, članak 8. Povelje valja shvatiti kao utjelovljenje postojećeg zakonodavstva o zaštiti podataka Europske unije. Stoga, osim što se u članku 8. stavku 1. Povelje izričito spominje pravo na zaštitu podataka, u članku 8. stavku 2. upućuje se i na ključna načela zaštite podataka. Naposljetku, člankom 8. stavkom 3. Povelje propisuje se da neovisno tijelo provodi kontrolu provedbe tih načela.

Donošenje Ugovora iz Lisabona prekretnica je u razvoju zakonodavstva o zaštiti podataka, ne samo zbog uzdizanja Povelje na razinu pravno obvezujućeg dokumenta primarnog prava nego i zbog osiguravanja prava na zaštitu osobnih podataka. To se pravo izričito utvrđuje u članku 16. UFEU-a, u dijelu Ugovora posvećenom općim načelima EU-a. Članak 16. također stvara novu pravnu osnovu kojom se EU-u dodjeljuje nadležnost donošenja zakona o pitanjima zaštite podataka. To je važno jer su se propisi EU-a o zaštiti podataka, osobito Direktiva o zaštiti podataka, prvobitno temeljili na pravnoj osnovi unutarnjeg tržišta i na potrebi za usklađivanjem nacionalnih zakona kako se slobodno kretanje podataka u EU-u ne bi ograničilo. Članak 16. UFEU-a sada pruža neovisnu pravnu osnovu za suvremen, sveobuhvatan pristup zaštiti podataka, koji obuhvaća sva pitanja u nadležnosti EU-a, uključujući policijsku i pravosudnu suradnju u kaznenim pitanjima. Člankom 16. UFEU-a također se potvrđuje da usklađenost s propisima o zaštiti podataka koji su doneseni u skladu s njime mora podlijeagati kontroli neovisnih nadzornih tijela. Članak 16. poslužio je kao pravna osnova za donošenje sveobuhvatne reforme propisa o zaštiti podataka 2016.,

27 EU (2012.), Povelja Europske unije o temeljnim pravima, SL 2012 C 326.

28 Vidjeti pročišćeni tekst Europskih zajednica (2012.), Ugovor o Europskoj uniji, SL 2012 C 326; i Europskih zajednica (2012.), UFEU, SL 2012 C 326.

odnosno Opće uredbe o zaštiti podataka i Direktive o zaštiti podataka za policiju i tijela kaznenog pravosuđa (vidjeti u nastavku).

Opća uredba o zaštiti podataka (OUZP)

Od 1995. do svibnja 2018. glavni pravni instrument EU-a u vezi sa zaštitom podataka bila je Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Direktiva o zaštiti podataka)²⁹. Donesena je 1995., u vrijeme kada je nekoliko država članica već donijelo nacionalne zakone o zaštiti podataka,³⁰ a proizšla je iz potrebe za usklađivanjem tih zakona kako bi se osigurali visoka razina zaštite i slobodan protok osobnih podataka među različitim državama članicama. Preduvjet za slobodno kretanje robe, kapitala, usluga i ljudi na unutarnjem tržištu bio je slobodan prijenos podataka koji se nije mogao ostvariti bez pouzdane i ujednačeno visoke razine zaštite podataka u državama članicama.

U Direktivi o zaštiti podataka odražavala su se, a često i proširivala načela zaštite podataka koja su već bila obuhvaćena nacionalnim zakonima i Konvencijom br. 108. U Direktivi je ostavljena mogućnost dodavanja instrumenata zaštite, koja je predviđena člankom 11. Konvencije br. 108. Uvođenje neovisnog nadzora u Direktivi kao instrumenta za bolju usklađenost s propisima o zaštiti podataka pokazalo se važnim doprinosom učinkovitim funkcioniranju europskog zakonodavstva o zaštiti podataka, stoga je taj instrument 2001. preuzet u pravu Vijeća Europe Dodatnim protokolom uz Konvenciju br. 108. To pokazuje usku povezanost i međusoban pozitivan utjecaj dvaju instrumenata tijekom godina.

Direktivom o zaštiti podataka uspostavljen je detaljan i sveobuhvatan sustav zaštite podataka u EU-u. Međutim, prema pravnom sustavu EU-a, direktive se ne primjenjuju izravno te se moraju prenijeti u nacionalne zakone država članica. Države članice pritom imaju diskrecijsku ovlast u prenošenju odredaba direktive. Iako se

29 Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL 1995 L 281.

30 Njemačka savezna država Hessen donijela je 1970. prvi zakon o zaštiti podataka u svijetu, koji se primjenjivao samo u toj državi. Švedska je 1973. donijela zakon *Datalagen*, Njemačka je 1976. donijela *Bundesdatenschutzgesetz*, a Francuska je 1977. donijela *Loi relatif à l'informatique, aux fichiers et aux libertés*. Ujedinjena Kraljevina donijela je Zakon o zaštiti podataka 1984. (engl. *Data Protection Act*), a Nizozemska je 1989. donijela *Wet Persoonregistraties*.

Direktivom nastojalo osigurati potpuno usklađivanje³¹ (i potpuna zaštita), u praksi se ona različito prenosila u pojedinim državama članicama. To je dovelo do postojanja različitih propisa o zaštiti podataka u EU-u te različitih definicija i tumačenja propisa u nacionalnim zakonima. Isto tako, razine provedbe i težina sankcija razlikovale su se među državama članicama. Naposljetku, od izrade nacрта Direktive sredinom 1990-ih došlo je do znatnih promjena informacijske tehnologije. Svi ti razlozi potaknuli su reformu zakonodavstva o zaštiti podataka u EU-u.

Reforma je dovela do donošenja Opće uredbe o zaštiti podataka u travnju 2016., nakon više godina intenzivnih rasprava. Rasprave o potrebi za modernizacijom propisa o zaštiti podataka u EU-u započele su 2009., kada je Komisija pokrenula javno savjetovanje o budućem pravnom okviru za temeljno pravo na zaštitu osobnih podataka. Komisija je objavila Prijedlog uredbe u siječnju 2012., čime je započet dug zakonodavni postupak pregovora između Europskog parlamenta i Vijeća Europske unije. Nakon donošenja, Opća uredba o zaštiti podataka omogućila je dvogodišnje prijelazno razdoblje. U potpunosti se počela primjenjivati od 25. svibnja 2018., a time je izvan snage stavljena Direktiva o zaštiti podataka.

Donošenjem Opće uredbe o zaštiti podataka 2016. modernizirano je zakonodavstvo EU-a o zaštiti podataka i omogućena zaštita temeljnih prava u kontekstu ekonomskih i društvenih izazova digitalnog doba. OUZP-om se čuvaju i razvijaju temeljna načela i prava ispitanika koja su utvrđena Direktivom o zaštiti podataka. Usto, Uredbom su uvedene nove obveze prema kojima organizacije moraju provoditi tehničku i integriranu zaštitu podataka, imenovati službenika za zaštitu podataka u određenim okolnostima, poštovati novo pravo na prenosivost podataka i pridržavati se načela odgovornosti. U skladu s pravom EU-a, uredbe su izravno primjenjive, što znači da nije potrebna provedba na nacionalnoj razini. Opća uredba o zaštiti podataka stoga pruža jedinstven skup pravila o zaštiti podataka na razini EU-a. Time se stvaraju dosljedna pravila o zaštiti podataka za cijeli EU i uspostavlja okruženje pravne sigurnosti od kojega koristi mogu imati gospodarski subjekti i pojedinci kao „ispitanici“.

Međutim, iako je Opća uredba o zaštiti podataka izravno primjenjiva, od država članica očekuje se da izmijene svoje postojeće nacionalno zakonodavstvo o zaštiti podataka radi potpunog usklađivanja s Uredbom, uz određene diskrecijske ovlasti koje se odnose na posebne odredbe iz uvodne izjave 10. Temeljna pravila i načela utvrđena Uredbom te snažna prava koja se njome dodjeljuju pojedincima čine

31 SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEDM) protiv Administración del Estado*, 24. studenoga 2011., t. 29.

znatan dio ovog priručnika i prikazana su u sljedećim poglavljima. Uredba uključuje sveobuhvatna pravila u vezi s teritorijalnim područjem primjene. Uredba se primjenjuje na poduzeća s poslovnim nastanom u EU-u te na voditelje obrade i izvršitelje obrade koji nemaju nastan u EU-u, a pružaju proizvode ili usluge subjektima podataka (ispitanicima) u EU-u ili nadziru njihovo ponašanje. Budući da nekoliko stranih tehnoloških poduzeća ima značajan udio na europskom tržištu i milijune potrošača u EU-u, primjena propisa EU-a o zaštiti podataka na te organizacije važna je za osiguravanje zaštite pojedinaca i ravnopravnih uvjeta poslovanja.

Zaštita podataka u području izvršavanja zakonodavstva – Direktiva (EU) 2016/680

Direktiva o zaštiti podataka koja je stavljena izvan snage pružala je sveobuhvatan sustav zaštite podataka. Taj je sustav dodatno proširen donošenjem Opće uredbe o zaštiti podataka. Iako je nekadašnja Direktiva o zaštiti podataka bila sveobuhvatna, njezino područje primjene bilo je ograničeno na aktivnosti koje pripadaju unutarnjem tržištu te aktivnosti javnih tijela koja ne sudjeluju u izvršavanju zakonodavstva. Stoga je bilo potrebno donošenje posebnih instrumenata radi postizanja nužne jasnoće i ravnoteže između zaštite podataka i drugih legitimnih interesa te radi suočavanja s izazovima koji su posebno relevantni za određene sektore. To se odnosi na propise kojima se uređuje obrada osobnih podataka koju obavljaju tijela zadužena za izvršavanje zakonodavstva.

Prvi pravni instrument EU-a kojim je uređeno ovo pitanje bila je Okvirna odluka Vijeća 2008/977/PUP o zaštiti osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima. Odredbe Odluke primjenjivale su se samo na policijske i pravosudne podatke prilikom razmjene među državama članicama. Domaća obrada osobnih podataka koju obavljaju tijela zadužena za izvršavanje zakonodavstva nije bila obuhvaćena područjem primjene Odluke.

To je ispravljeno Direktivom (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka,³² koja se naziva Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa. Direktiva je donesena istodobno s Općom uredbom o zaštiti

32 Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka, SL L 119, 4. svibnja 2016.

podataka. Njome je izvan snage stavljena Okvirna odluka 2008/977/PUP i uspostavljen je sveobuhvatan sustav zaštite osobnih podataka u kontekstu izvršavanja zakonodavstva, a istodobno su prepoznate posebnosti obrade podataka povezane s javnom sigurnošću. Dok se Općom uredbom o zaštiti podataka utvrđuju opća pravila za zaštitu pojedinaca u pogledu obrade njihovih osobnih podataka i osiguravanja slobodnog protoka takvih podataka unutar EU-a, Direktivom se utvrđuju posebna pravila za zaštitu podataka u područjima pravosudne suradnje u kaznenim pitanjima i policijske suradnje. Direktiva (EU) 2016/680 primjenjivat će se na svaki slučaj u kojem neko nadležno tijelo obrađuje osobne podatke u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela. Kada nadležna tijela obrađuju osobne podatke u svrhe izvan prethodno spomenutih, primjenjivat će se opći sustav Opće uredbe o zaštiti podataka. Za razliku od prethodnog propisa (Okvirna odluka Vijeća 2008/977/PUP), područje primjene Direktive (EU) 2016/680 proširuje se na nacionalnu obradu osobnih podataka koju obavljaju tijela za izvršavanje zakonodavstva i nije ograničeno na razmjenu takvih podataka među državama članicama. Usto, Direktivom se nastoji uspostaviti ravnoteža između prava pojedinaca i legitimnih ciljeva obrade u sigurnosne svrhe.

U tu se svrhu u Direktivi potvrđuju pravo na zaštitu osobnih podataka i temeljna načela koja bi trebala obuhvaćati obradu podataka, koja su usko povezana s pravilima i načelima utvrđenima u Općoj uredbi o zaštiti podataka. Prava pojedinaca i propisane obveze voditelja obrade, primjerice u vezi sa sigurnošću podataka, tehničkom i integriranom zaštitom podataka i obavještanjem u slučaju povrede podataka, slični su pravima i obvezama iz Opće uredbe o zaštiti podataka. U Direktivi se također nastoje razmotriti i riješiti novi, ozbiljni tehnološki izazovi koji mogu imati posebno težak utjecaj na pojedince, kao što su metode izrade profila koje upotrebljavaju tijela zadužena za izvršavanje zakonodavstva. U načelu se mora zabraniti donošenje odluka isključivo na temelju automatizirane obrade podataka, uključujući izradu profila³³. Odluke se jednako tako ne smiju temeljiti ni na osjetljivim podacima. Za spomenuta načela mogu vrijediti određene iznimke utvrđene u Direktivi. Također, obrada ne smije dovesti do diskriminacije bilo koje osobe³⁴.

Direktiva također sadržava odredbe kojima se osigurava odgovornost voditelja obrade. Oni moraju imenovati službenika za zaštitu podataka koji će nadzirati usklađenost s propisima o zaštiti podataka, savjetovati tijelo i zaposlenike koji provode obradu podataka i informirati ih o njihovim obvezama te surađivati s nadzornim tijelom. Obrada osobnih podataka u sektoru policije i kaznenog prava sada podliježe

33 Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa, članak 11. stavak 1.

34 *Ibid.*, članak 11. stavci 2. i 3.

nadzoru neovisnih nadzornih tijela. I opći pravni sustav zaštite podataka i poseban sustav zaštite podataka koji se odnosi na tijela za izvršavanje zakonodavstva i kaznena pitanja moraju u jednakoj mjeri biti usklađeni sa zahtjevima Povelje EU-a o temeljnim pravima.

Posebni sustav obrade podataka u kontekstu policije i pravosudne suradnje, uspostavljen Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa, detaljno je opisan u [poglavlju 8](#).

Direktiva o privatnosti i elektroničkim komunikacijama

Utvrđivanje posebnih propisa za zaštitu podataka smatralo se potrebnim i u sektoru elektroničkih komunikacija. Zbog razvoja interneta te fiksne i mobilne telefonije bilo je važno osigurati poštovanje prava korisnika na privatnost i povjerljivost. Direktivom 2002/58/EZ³⁵ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) utvrđuju se pravila o sigurnosti osobnih podataka u tim mrežama, obavješćivanju u slučaju povrede osobnih podataka i povjerljivosti komunikacija.

Kad je riječ o sigurnosti, pružatelji elektroničkih komunikacijskih usluga moraju, među ostalim, osigurati da je pristup osobnim podacima ograničen isključivo na ovlaštene osobe i poduzeti mjere za sprečavanje uništavanja, gubitka ili nehotičnog oštećenja osobnih podataka³⁶. Ako postoji poseban rizik od povrede sigurnosti javnih komunikacijskih mreža, operateri moraju obavijestiti pretplatnike o tom riziku³⁷. Ako dođe do povrede sigurnosti unatoč poduzetim sigurnosnim mjerama, operateri moraju obavijestiti nadležno nacionalno tijelo koje ima zadatak primjene i provedbe Direktive u slučaju povrede osobnih podataka. Operateri ponekad moraju obavijestiti i pojedince o povredi osobnih podataka, primjerice u slučaju kada bi takva povreda mogla negativno utjecati na njihove osobne podatke ili privatnost³⁸. Za očuvanje povjerljivosti komunikacije potrebno je u načelu zabraniti slušanje, prisluškivanje, pohranjivanje ili bilo koji oblik nadzora ili presretanja komunikacije i metapodataka. Direktivom se također zabranjuju neželjene komunikacije (koje se često nazivaju *spam*), osim ako korisnici ne daju pristanak za to, a ona sadržava i pravila

35 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija, SL L 201 (Direktiva o privatnosti i elektroničkim komunikacijama).

36 Direktiva o privatnosti i elektroničkim komunikacijama, članak 4. stavak 1.

37 *Ibid.*, članak 4. stavak 2.

38 *Ibid.*, članak 4. stavak 3.

o pohranjivanju „kolačića” na računalima i drugim uređajima. Ove ključne negativne obveze jasno upućuju na to da je povjerljivost komunikacije snažno povezana sa zaštitom prava na poštovanje privatnog života, sadržanog u članku 7. Povelje, i prava na zaštitu osobnih podataka, sadržanog u članku 8. Povelje.

U siječnju 2017. Komisija je objavila Prijedlog uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama, koja bi trebala zamijeniti Direktivu o privatnosti i elektroničkim komunikacijama. Reformom se odredbe kojima se uređuju elektroničke komunikacije nastoje uskladiti s novim sustavom zaštite podataka koji je uspostavljen Općom uredbom o zaštiti podataka. Nova uredba bit će izravno primjenjiva u cijelom EU-u. Svi pojedinci uživat će jednaku razinu zaštite svojih elektroničkih komunikacija, dok će telekomunikacijski operateri i društva ostvariti korist od jasnoće, pravne sigurnosti i postojanja jedinstvenog skupa pravila na području cijelog EU-a. Predloženi propisi o povjerljivosti elektroničkih komunikacija primjenjivat će se i na nove sudionike na tržištu elektroničkih komunikacijskih usluga koje nisu obuhvaćene Direktivom o privatnosti i elektroničkim komunikacijama. Direktivom su obuhvaćeni samo tradicionalni pružatelji telekomunikacijskih usluga. Budući da dolazi do snažnog širenja upotrebe usluga kao što su Skype, WhatsApp, Facebook Messenger i Viber za slanje poruka ili pozivanje, te tzv. *over-the-top* (OTT) usluge sada će biti obuhvaćene područjem primjene uredbe i morat će biti u skladu s njezinim zahtjevima u pogledu zaštite, privatnosti i sigurnosti podataka. U trenutku objave ovog priručnika zakonodavni postupak donošenja propisa o e-privatnosti još je bio u tijeku.

Uredba (EZ) br. 45/2001

Budući da se Direktiva o zaštiti podataka mogla primjenjivati samo na države članice EU-a, bio je potreban dodatni pravni instrument kako bi se osigurala zaštita podataka pri obradi osobnih podataka u institucijama i tijelima Europske unije. To je učinjeno Uredbom (EZ) br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (Uredba o zaštiti podataka u institucijama Europske unije)³⁹.

Uredba (EZ) br. 45/2001 slijedi načela općeg sustava zaštite podataka EU-a i njome se ta načela primjenjuju na obradu podataka koju provode institucije i tijela EU-a pri obavljanju svojih funkcija. Usto, njome se uspostavlja nezavisno nadzorno tijelo koje

³⁹ Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

nadzire primjenu njezinih odredbi – Europski nadzornik za zaštitu podataka (EDPS). EDPS-u su dodijeljene nadzorne ovlasti i dužnost nadzora nad obradom osobnih podataka u institucijama i tijelima EU-a, kao i zaprimanje i istraživanje pritužbi na navodna kršenja propisa o zaštiti podataka. EDPS također savjetuje institucije i tijela EU-a o svim pitanjima koja se odnose na zaštitu osobnih podataka, od prijedloga novog zakonodavstva do izrade nacrtu internih pravila o obradi podataka.

U siječnju 2017. Europska komisija predstavila je Prijedlog nove uredbe o obradi podataka u institucijama EU-a, kojom će se postojeća Uredba staviti izvan snage. Kao i u slučaju reforme Direktive o privatnosti i elektroničkim komunikacijama, reformom Uredbe (EZ) br. 45/2001 njezine će se odredbe modernizirati i uskladiti s novim sustavom zaštite podataka koji je uspostavljen Općom uredbom o zaštiti podataka.

Uloga Suda Europske unije (SEU)

SEU je nadležan za utvrđivanje je li neka država članica ispunila svoje obveze na temelju zakonodavstva EU-a o zaštiti podataka te za tumačenje zakonodavstva EU-a kako bi se osigurala njegova učinkovita i ujednačena primjena u svim državama članicama. Od donošenja Direktive o zaštiti podataka 1995. akumulirala se znatna sudska praksa kojom se pojašnjavaju područje primjene i značenje načela zaštite podataka te temeljno pravo na zaštitu osobnih podataka zajamčeno člankom 8. Povelje. Iako je Direktiva stavljena izvan snage te je sada na snazi novi pravni instrument, tj. Opća uredba o zaštiti podataka, prethodna sudska praksa i dalje je relevantna i važeća za tumačenje i primjenu načela EU-a o zaštiti podataka s obzirom na to da su temeljna načela i koncepti Direktive o zaštiti podataka zadržani u OUZP-u.

1.2. Ograničenja prava na zaštitu osobnih podataka

Ključne točke

- Pravo na zaštitu osobnih podataka nije apsolutno pravo. Ono se može ograničiti ako je to potrebno radi ostvarenja određenog cilja od općeg interesa ili radi zaštite prava i sloboda drugih osoba.
- Uvjeti za ograničenje prava na poštovanje privatnog života i zaštitu osobnih podataka navedeni su u članku 8. EKLJP-a i članku 52. stavku 1. Povelje. Oni su razrađeni i protumačeni u okviru sudske prakse ESLJP-a i SEU-a.

- Prema zakonodavstvu o zaštiti podataka Vijeća Europe, obrada osobnih podataka predstavlja zakonito miješanje u pravo na poštovanje privatnog života i može se provoditi samo pod sljedećim uvjetima:
 - u skladu je sa zakonom,
 - ima legitiman cilj,
 - poštuje suštinu temeljnih prava i sloboda,
 - nužna je i proporcionalna u demokratskom društvu radi postizanja legitimne svrhe.
- Pravnim poretom EU-a postavljaju se slični uvjeti ograničenja ostvarivanja temeljnih prava zaštićenih Poveljom. Ograničenje bilo kojeg temeljnog prava, uključujući pravo na zaštitu osobnih podataka, može biti zakonito samo pod sljedećim uvjetima:
 - u skladu je sa zakonom,
 - poštuje suštinu tog prava,
 - nužno je, i to nakon što se podvrgne kriteriju proporcionalnosti, te
 - ispunjava cilj od općeg interesa koji priznaje EU ili pak potrebu za zaštitom prava drugih.

Temeljno pravo na zaštitu osobnih podataka sadržano u članku 8. Povelje nije apsolutno pravo, „već se mora razmatrati u vezi s njegovom funkcijom u društvu”⁴⁰. U članku 52. stavku 1. Povelje tako se potvrđuje mogućnost nametanja ograničenja pri provedbi prava, poput onih iz članaka 7. i 8. Povelje, pod uvjetom da su takva ograničenja zakonita, da poštuju suštinu tih prava i sloboda te da su sukladno načelu proporcionalnosti nužna i da istinski ispunjavaju ciljeve od općeg interesa koje je prepoznao EU ili pak potrebu za zaštitom tuđih prava i sloboda⁴¹. Slično tome, u sustavu EKLJP-a zaštita podataka zajamčena je člankom 8., a provedba tog prava može biti ograničena kada je to potrebno za ostvarenje legitimnog cilja. U ovom poglavlju obuhvaćeni su uvjeti za miješanje u spomenuto pravo na temelju EKLJP-a kako se tumače u okviru sudske prakse ESLJP-a, kao i uvjeti za zakonita ograničenja u skladu s člankom 52. Povelje.

40 Vidjeti, primjerice, SEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010., t. 48.

41 *Ibid.*, t. 50.

1.2.1. Zahtjevi iz Europske konvencije o ljudskim pravima (EKLJP) koje je potrebno zadovoljiti kako bi miješanje bilo opravdano

Obrada osobnih podataka može se smatrati miješanjem u pravo na poštovanje privatnog života ispitanika, koje je zaštićeno člankom 8. EKLJP-a⁴². Kako je prethodno objašnjeno (vidjeti dio 1.1.1. i dio 1.1.4.), za razliku od pravnog poretka EU-a, EKLJP-om se zaštita osobnih podataka ne utvrđuje kao zasebno temeljno pravo. Zaštita osobnih podataka u sklopu Konvencije zapravo je dio prava zaštićenih u okviru prava na poštovanje privatnog života. Stoga ne bi svaka radnja koja uključuje obradu osobnih podataka bila obuhvaćena područjem primjene članka 8. EKLJP-a. Da bi se primjenjivao članak 8., prvo je potrebno utvrditi je li narušen neki privatni interes ili privatni život osobe. ESLJP u svojoj sudskoj praksi pojam „privatnog života” smatra konceptom širokog značenja, koji obuhvaća čak i neke aspekte profesionalnog života i ponašanja u javnosti. Također je presuđivao da je zaštita osobnih podataka važan dio prava na poštovanje privatnog života. Međutim, unatoč širokom tumačenju privatnog života, ne ugrožavaju sve vrste obrade podataka same po sebi prava zaštićena člankom 8.

Kada ESLJP smatra da predmetni postupak obrade utječe na pravo pojedinca na poštovanje privatnog života, preispitat će je li takvo miješanje u pravo opravdano. Pravo na poštovanje privatnog života nije apsolutno pravo, već se mora odvagovati i uskladiti s drugim legitimnim interesima i pravima, bilo da je riječ o pravima i interesima drugih osoba (privatnim interesima) ili pravima i interesima društva u cjelini (javnim interesima).

Skupni uvjeti u kojima miješanje može biti opravdano jesu sljedeći:

U skladu sa zakonom

Prema sudskoj praksi Europskog suda za ljudska prava, miješanje je u skladu sa zakonom ako se temelji na odredbi nacionalnog zakonodavstva koje ima određene odlike. Zakon mora biti „dostupan dotičnim osobama i njegovi učinci moraju biti predvidljivi”⁴³. Pravilo je predvidljivo „ako je formulirano dovoljno precizno da svaki

⁴² ESLJP, *S. i Marper protiv Ujedinjene Kraljevine* [VV], br. 30562/04 i 30566/04, 4. prosinca 2008., t. 67.

⁴³ ESLJP, *Amann protiv Švicarske* [VV], br. 27798/95, 16. veljače 2000., t. 50.; vidjeti također ESLJP, *Kopp protiv Švicarske*, br. 23224/94, 25. ožujka 1998., t. 55. i ESLJP, *lordachi i drugi protiv Moldavije*, br. 25198/02, 10. veljače 2009., t. 50.

pojedinaac – uz, po potrebi, odgovarajuće savjetovanje – može regulirati svoje postupanje⁴⁴. Nadalje, „[s]tupanj preciznosti koji zakon mora imati u tom pogledu ovisi o konkretnom slučaju⁴⁵“.

Primjeri: U predmetu *Rotaru protiv Rumunjske*⁴⁶ tužitelj je naveo da Obavještajna služba Rumunjske krši njegova prava na poštovanje privatnog života zbog toga što čuva i upotrebljava dosje s njegovim osobnim podacima. Europski sud za ljudska prava utvrdio je da, iako je prema rumunjskom zakonu dopušteno prikupljanje informacija koje utječu na nacionalnu sigurnost te njihovo bilježenje i arhiviranje u tajnim spisima, granice za primjenu tih ovlasti nisu propisane, već ih određuju nadležna tijela. Na primjer, nacionalnim zakonodavstvom nisu definirane vrste informacija koje se smiju obrađivati, kategorije ljudi nad kojima se smiju provoditi mjere nadzora, okolnosti u kojima se takve mjere smiju provoditi ni postupak koji pri tome treba slijediti. Zbog toga je ESLJP zaključio da nacionalno zakonodavstvo nije bilo u skladu sa zahtjevom predvidljivosti iz članka 8. Europske konvencije o ljudskim pravima te da je taj članak prekršen.

U predmetu *Taylor-Sabori protiv Ujedinjene Kraljevine*⁴⁷ tužitelj je bio podvrgnut nadzoru policije. Koristeći se „klonom“ tužiteljeva dojavljivača policija je presretala poruke koje je primao. Tužitelj je nakon toga uhićen i optužen za zavjeru radi nabave kontrolirane droge. Tužiteljstvo je optužbe protiv tužitelja dijelom temeljilo na zapisima poruka iz dojavljivača koji su nastali u isto vrijeme, koje je policija transkribirala. Međutim, u trenutku kad se tužitelju sudilo, britanskim zakonodavstvom nije bilo regulirano presretanje komunikacije privatnim telekomunikacijskim sustavima. Miješanje u njegova prava stoga nije bilo „u skladu sa zakonom“. ESLJP je zaključio da je time prekršen članak 8. Konvencije.

44 ESLJP, *Amann protiv Švicarske* [VV], br. 27798/95, 16. veljače 2000., t. 56.; vidjeti također ESLJP, *Malone protiv Ujedinjene Kraljevine*, br. 8691/79, 2. kolovoza 1984., t. 66.; ESLJP, *Silver i dr. protiv Ujedinjene Kraljevine*, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983., t. 88.

45 ESLJP, *Sunday Times protiv Ujedinjene Kraljevine*, br. 6538/74, 26. travnja 1979., t. 49.; vidjeti također ESLJP, *Silver i dr. protiv Ujedinjene Kraljevine*, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983., t. 88.

46 ESLJP, *Rotaru protiv Rumunjske* [VV], br. 28341/95, 4. svibnja 2000., t. 57.; vidjeti također ESLJP, *Udruženje za europsku integraciju i ljudska prava i Ekimdzhiiev protiv Bugarske*, br. 62540/00, 28. lipnja 2007.; ESLJP, *Shimovolos protiv Rusije*, br. 30194/09, 21. lipnja 2011. i ESLJP, *Vetter protiv Francuske*, br. 59842/00, 31. svibnja 2005.

47 ESJLP, *Taylor-Sabori protiv Ujedinjene Kraljevine*, br. 47114/99, 22. listopada 2002.

Predmet *Vukota-Bojić protiv Švicarske*⁴⁸ odnosio se na tajni nadzor podnositeljice zahtjeva za socijalno osiguranje koji su provodili privatni istražitelji koje je angažiralo njezino osiguravajuće društvo. ESLJP je zaključio da iako je predmetnu mjeru nadzora u tužbi naručilo privatno osiguravajuće društvo, tom je društvu država dala pravo da pruža povlastice koje proizlaze iz obveznog zdravstvenog osiguranja i da naplaćuje premije osiguranja. Država se ne može osloboditi odgovornosti na temelju Konvencije tako da svoje obveze prenese na privatna tijela ili pojedince. Da bi miješanje u prava iz članka 8. EKLJP-a bilo „u skladu sa zakonom“, nacionalnim zakonodavstvom morale su biti propisane odgovarajuće mjere zaštite od zlouporabe. U navedenom predmetu ESLJP je zaključio da je došlo do kršenja članka 8. Konvencije jer u nacionalnom zakonodavstvu nije bilo dovoljno jasno navedeno područje primjene i način provedbe ovlasti za provođenje tajnog nadzora osigurane osobe koje su dodijeljene osiguravajućim društvima koja djeluju kao javna tijela u sporovima vezana za osiguranja. Točnije, zakonodavstvo nije sadržavalo dostatne mjere zaštite od zlouporabe.

Legitimna svrha

Legitimna svrha može se odnositi ili na spomenute javne interese ili na zaštitu prava i sloboda drugih. U skladu s člankom 8. stavkom 2. EKLJP-a, legitimne svrhe koje bi mogle opravdati miješanje u prava pojedinca jesu interesi državne sigurnosti, javni red i mir ili gospodarska dobrobit zemlje, sprečavanje nereda ili zločina, zaštita zdravlja ili morala te zaštita prava i sloboda drugih.

Primjer: U predmetu *Peck protiv Ujedinjene Kraljevine*⁴⁹ tužitelj je pokušao počiniti samoubojstvo na ulici tako što si je prerezao zapešća, a nije bio svjestan da ga se snima kamerom televizije zatvorenog kruga (CCTV). Policija je gledala snimke kamera CCTV-a i spasila ga, nakon čega je snimke prosljedila medijima, koji su ih objavili bez zamagljivanja lica tužitelja. ESLJP je zaključio da nije bilo relevantnih ni dostatnih razloga kojima bi se opravdalo izravno otkrivanje snimki javnosti bez privole tužitelja ili prikrivanja njegova identiteta. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

⁴⁸ ESLJP, *Vukota-Bojić protiv Švicarske*, br. 61838/10, 18. listopada 2016., t. 77.

⁴⁹ ESLJP, *Peck protiv Ujedinjene Kraljevine*, br. 44647/98, 28. siječnja 2003., t. 85.

Nužnost u demokratskom društvu

ESLJP je istaknuo da „pojam nužnosti podrazumijeva da je miješanje odgovor na neizbježnu potrebu društva i naročito da je razmjerno legitimnoj svrsi koja se nastoji ispuniti”⁵⁰. Prilikom ocjenjivanja je li neka mjera nužna da bi se ispunila neizbježna potreba društva, ESLJP preispituje njezinu relevantnost i primjerenost s obzirom na cilj koji se nastoji ostvariti. U tu svrhu može razmotriti pokušava li se miješanjem riješiti problem koji bi inače imao štetan učinak na društvo, postoje li dokazi da se miješanjem može ublažiti takav štetan učinak te koja su šira društvena stajališta o tom pitanju⁵¹. Primjerice, prikupljanjem i pohranjivanjem osobnih podataka određenih pojedinaca za koje se pokaže da imaju veze s terorističkim pokretima sigurnosne bi se službe miješale u pravo pojedinaca na poštovanje privatnog života, no takve radnje ujedno služe i ozbiljnoj, neizbježnoj društvenoj potrebi: nacionalnoj sigurnosti i borbi protiv terorizma. Da bi se ispunio kriterij „nužnosti”, miješanje također mora biti proporcionalno. U sudskoj praksi ESLJP-a proporcionalnost je obuhvaćena konceptom nužnosti. Da bi miješanje u prava zaštićena EKLJP-om bilo proporcionalno, ono ne smije izlaziti izvan okvira onoga što je nužno za ispunjenje legitimne svrhe koja se nastoji ostvariti. Važni čimbenici koje treba uzeti u obzir prilikom utvrđivanja proporcionalnosti jesu opseg miješanja, prvenstveno broj osoba koje će time biti zahvaćene, te zaštitne mjere ili upozorenja uspostavljena kako bi se ograničio njegov opseg ili štetni učinci na prava pojedinaca⁵².

Primjer: U predmetu *Khelili protiv Švicarske*⁵³ policija je provodeći provjeru utvrdila da tužiteljica posjeduje posjetnice na kojima je pisalo: „Simpatična, zgodna žena u kasnim tridesetima želi upoznati muškarca da se povremeno sastanu uz piće ili zajedno izađu. Telefonski br. [...]”. Tužiteljica se žalila da ju je policija nakon pronalaska posjetnice u svojoj evidenciji zapisala kao prostitutku, iako je ona uporno tvrdila da se time ne bavi. Tužiteljica je zatražila brisanje riječi „prostitutka” iz računalne evidencije policije. ESLJP je u načelu ustvrdio da zadržavanje osobnih podataka pojedinca zbog mogućnosti da ta osoba poćini drugo kazneno djelo u određenim okolnostima može biti proporcionalno. Međutim, u slučaju tužiteljice tvrdnja o navodnoj nezakonitoj prostituciji doimala se previše nejasnom i općenitom te nije bila potkrijepljena

50 ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987., t. 58.

51 Radna skupina za zaštitu podataka iz članka 29. (Radna skupina iz članka 29.) (2014.), *Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, Bruxelles, 27. veljače 2014., str. 7.–8.

52 *Ibid.*, str. 9.–11.

53 ESLJP, *Khelili protiv Švicarske*, br. 16188/07, 18. listopada 2011.

konkretnim činjenicama jer ona nikada nije bila osuđena za nezakonitu prostituciju, pa uvjet „neizbježne društvene potrebe“ u smislu članka 8. Konvencije nije bio ispunjen. Smatrajući da su nadležna tijela odgovorna za dokazivanje točnosti pohranjenih podataka o tužiteljici i uzimajući u obzir ozbiljnost narušavanja prava tužiteljice, ESLJP je presudio da dugotrajno zadržavanje riječi „prostitutka“ u policijskoj evidenciji nije bilo nužno u demokratskom društvu. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Primjer: U predmetu *S. i Marper protiv Ujedinjene Kraljevine*⁵⁴ oba su tužitelja uhićena i optužena za kaznena djela. Policija je uzela njihove otiske prstiju i uzorke DNK-a, kako je propisano Zakonom o policiji i dokazima u kaznenom postupku Ujedinjene Kraljevine (engl. *Police and Criminal Evidence Act*). Tužitelji za ta kaznena djela nisu bili osuđeni: jedan od njih oslobođen je na sudu, a kazneni je postupak protiv drugoga obustavljen. Unatoč tome policija je njihove otiske prstiju, DNK profile i stanične uzorke zadržala i pohranila u bazi podataka, a nacionalnim zakonodavstvom dopušteno je njihovo zadržavanje bez vremenskog ograničenja. Ujedinjena Kraljevina tvrdila je da je zadržavanje materijala pomoglo u otkrivanju budućih počinitelja kaznenih djela te da je tako nastojala ostvariti legitiman cilj prevencije i otkrivanja zločina, no ESLJP je to smatrao neopravdanim miješanjem u pravo tužitelja na poštovanje privatnog života. Istaknuo je da prema temeljnim načelima zaštite podataka zadržavanje osobnih podataka mora biti proporcionalno s obzirom na svrhu prikupljanja te da razdoblja zadržavanja moraju biti ograničena. ESLJP je prihvatio argument da je proširivanje baze podataka na DNK profile i osuđenih osoba i svih pojedinaca koji su osumnjičeni, no ne i osuđeni, moglo pridonijeti otkrivanju i prevenciji kaznenih djela u Ujedinjenoj Kraljevini. Međutim, bio je „iznenađen sveobuhvatnim i neselektivnim karakterom ovlasti zadržavanja podataka“⁵⁵.

S obzirom na brojne genetske i zdravstvene informacije sadržane u staničnim uzorcima, miješanje u pravo tužitelja na privatni život bilo je posebno ozbiljno. Otisci prstiju i uzorci mogli su se uzimati od uhićenika i neograničeno zadržavati u policijskoj bazi podataka neovisno o prirodi i težini počinjenog djela, čak i za manje prekršaje za koje nije predviđena zatvorska kazna. Osim toga, mogućnost da se podaci o oslobođenim pojedincima izbrišu iz baze podataka bila je ograničena. Naposljetku, ESLJP je posebno uzeo u obzir činjenicu da je jedan od tužitelja u trenutku uhićenja imao jedanaest godina. Zadržavanje

54 ESLJP, *S. i Marper protiv Ujedinjene Kraljevine* [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.

55 *Ibid.*, t. 119.

osobnih podataka maloljetnika koji nije osuđen može biti posebno štetno zbog njegove osjetljivosti i važnosti njegova razvoja i integracije u društvo⁵⁶. Sud je donio jednoglasnu odluku da je zadržavanje podataka predstavljalo neproporcionalno miješanje u pravo na privatni život koje se ne može smatrati nužnim u demokratskom društvu.

Primjer: U predmetu *Leander protiv Švedske*⁵⁷ ESLJP je presudio da tajna provjera osoba koje se prijavljuju za zaposlenje na radnim mjestima važnima za nacionalnu sigurnost nije sama po sebi u suprotnosti sa zahtjevom nužnosti u demokratskom društvu. Posebne zaštitne mjere propisane nacionalnim zakonodavstvom za zaštitu interesa ispitanika – na primjer kontrole koje provode parlament i ministar pravosuđa za pravosuđe – dovele su do zaključka ESLJP-a da je švedski sustav za kontrolu osoblja ispunio zahtjeve iz članka 8. stavka 2. EKLJP-a. Imajući na umu da je imala na raspolaganju velik raspon procjena, tužena država s pravom je smatrala da su u tužiteljevu slučaju interesi nacionalne sigurnosti bili važniji od pojedinačnih. ESLJP je stoga zaključio da nije došlo do kršenja članka 8. Konvencije.

1.2.2. Uvjeti za zakonita ograničenja u skladu s Poveljom Europske unije o temeljnim pravima

Struktura i tekst Povelje razlikuju se od strukture i teksta Europske konvencije o ljudskim pravima. U Povelji se ne javlja koncept miješanja u zajamčena prava, no u njoj je sadržana odredba o ograničenju/ima pri ostvarivanju prava i sloboda priznatih Poveljom.

Prema članku 52. stavku 1., ograničenja pri ostvarivanju prava i sloboda priznatih Poveljom i, u skladu s time, pri ostvarivanju prava na zaštitu osobnih podataka prihvatljiva su samo pod sljedećim uvjetima:

- propisana su zakonom,
- poštuju suštinu prava na zaštitu podataka,

⁵⁶ *Ibid.*, t. 124.

⁵⁷ ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987., t. 59. i 67.

- nužna su prema načelu proporcionalnosti⁵⁸, te
- ispunjavaju ciljeve od općeg interesa koje priznaje Unija ili potrebu za zaštitom prava i sloboda drugih.

Budući da je zaštita osobnih podataka zasebno i samostalno temeljno pravo u pravnom poretku EU-a zaštićeno člankom 8. Povelje, svaka obrada osobnih podataka sama je po sebi miješanje u to pravo. Nevažno je jesu li ti osobni podaci povezani s privatnim životom pojedinca, jesu li osjetljivi i je li ispitanicima bilo kako uzrokovana neugodnost. Da bi bilo zakonito, miješanje mora ispunjavati sve uvjete navedene u članku 52. stavku 1. Povelje.

Propisano zakonom

Ograničenja prava na zaštitu osobnih podataka moraju biti propisana zakonom. Ovim se uvjetom podrazumijeva da se ograničenja moraju temeljiti na pravnoj osnovi koja je dovoljno pristupačna i predvidljiva te dovoljno precizno formulirana kako bi pojedincima omogućila da razumiju svoje obveze i kontroliraju svoje postupke. Pravna osnova također mora pružati jasnu definiciju područja primjene i načina izvršavanja ovlasti nadležnih tijela kako bi se pojedinci zaštitili od proizvoljnog miješanja. Takvo tumačenje slično je zahtjevu „zakonitog miješanja“ iz sudske prakse ESLJP-a⁵⁹, a raspravlja se i o tome da značenje izraza „propisano zakonom“ koji se upotrebljava u Povelji treba biti jednako značenju koje taj izraz ima u kontekstu EKLJP-a⁶⁰. Sudska praksa ESLJP-a, a posebno koncept „kvalitete zakona“ koji je razvio tijekom godina, važna je stavka koju SEU mora uzeti u obzir prilikom tumačenja područja primjene članka 52. stavka 1. Povelje⁶¹.

Poštovanje suštine prava

U pravnom poretku EU-a svako ograničenje temeljnih prava zaštićenih Poveljom mora poštovati suštinu tih prava. To znači da se ne mogu opravdati ograničenja koja

58 Za procjenu nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka vidjeti: EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mjera), Bruxelles, 11. travnja 2017.

59 EDPS (2017.), Paket alata za određivanje nužnosti mjera, Bruxelles, 11. travnja 2017., str. 4.; vidjeti i SEU, *Mišljenje 1/15 Suda* [VV], 26. srpnja 2017.

60 SEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona, Petera Bricea, Geoffreya Lewisa*, *Mišljenje nezavisnog odvjetnika Henrika Saugmandsgaarda Øea*, od 19. srpnja 2016., t. 140.

61 SEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, *Mišljenje nezavisnog odvjetnika Pedra Cruza Villalóna*, od 14. travnja 2011., t. 100.

su toliko opsežna i ozbiljna da zbog njih neko temeljno pravo gubi svoj osnovni smisao. Ako je suština prava ugrožena, ograničenje se mora smatrati nezakonitim i nije potrebna daljnja procjena služi li ono cilju od općeg interesa te zadovoljava li kriterije nužnosti i proporcionalnosti.

Primjer: Predmet *Schrems*⁶² odnosio se na zaštitu pojedinaca u pogledu prijenosa njihovih osobnih podataka u treće zemlje, u ovom slučaju u Sjedinjene Američke Države. Schrems, austrijski državljanin i dugogodišnji korisnik društvene mreže Facebook, podnio je pritužbu irskom nadležnom tijelu za zaštitu podataka kako bi javno osudilo prijenos njegovih osobnih podataka iz irske podružnice društva Facebook u društvo Facebook, Inc. te na poslužitelje u SAD-u, gdje su se podaci obrađivali. Tvrdio je da zakoni i praksa u SAD-u ne pružaju dostatnu zaštitu osobnih podataka koji se prenose na državno područje SAD-a kada se uzmu u obzir informacije koje je 2013. američki zviždač Edward Snowden razotkrio u vezi s aktivnostima nadzora američkih obavještajnih službi. Snowden je obznanio da je američka Nacionalna sigurnosna agencija (engl. *National Security Agency*) imala izravan pristup računalnim poslužiteljima društava kao što je Facebook te je mogla čitati sadržaj razgovora i privatnih poruka.

Prijenosi podataka u SAD temeljili su se na Odluci Komisije o primjerenosti donesenoj 2000., kojom su omogućeni prijenosi društvima u SAD-u koja su sama potvrdila da će štititi osobne podatke prenesene iz EU-a i pridržavati se tzv. načela „sigurne luke“. Kada je predmet iznesen pred SEU-om, on je preispitao valjanost Odluke Komisije u kontekstu Povelje. Podsjetio je da zaštita temeljnih prava u EU-u zahtijeva da se izuzeća i ograničenja tih prava primjenjuju samo ako su strogo nužna. SEU je smatrao da propis koji javnim tijelima omogućuje općenit pristup sadržaju elektroničkih komunikacija „povređuje bitan sadržaj temeljnog prava na poštovanje privatnog života koje je zajamčeno u članku 7. Povelje“. Pravo bi izgubilo smisao ako bi javna tijela SAD-a bila ovlaštena za bezrazložno pristupanje komunikacijama, bez objektivnog opravdanja koje se temelji na konkretnim razlozima nacionalne sigurnosti ili prevencije kaznenih djela koja se povezuju s konkretnim pojedincem te bez osiguravanja odgovarajućih mjera zaštite od zlouporabe ovlasti za te nadzorne prakse.

62 SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VV], 6. listopada 2015.

Usto, SEU je istaknuo da „propis koji pojedincima ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose ili radi ispravka ili brisanja takvih podataka” nije u skladu s temeljnim pravom na djelotvornu sudsku zaštitu (članak 47. Povelje). Stoga Odlukom o sigurnoj luci nije osigurana razina zaštite temeljnih prava u SAD-u koja bi u osnovi bila jednakovrijedna onoj koja je zajamčena unutar EU-a na temelju direktive tumačene u kontekstu Povelje. SEU je stoga Odluku proglasio nevaljanom⁶³.

Primjer: U predmetu *Digital Rights Ireland*⁶⁴ SEU je ispitao usklađenost Direktive 2006/24/EZ (Direktiva o zadržavanju podataka) s člancima 7. i 8. Povelje. Direktivom se pružateljima elektroničkih komunikacijskih usluga odredila obveza zadržavanja podataka o prometu i lokaciji najmanje šest mjeseci, a najviše 24 mjeseca, te omogućivanja nadležnim nacionalnim tijelima da pristupe tim podacima radi sprečavanja, istrage, otkrivanja i progona teških kaznenih djela. Direktivom nije dopušteno zadržavanje sadržaja elektroničkih komunikacija. SEU je istaknuo da podaci koje pružatelji usluga moraju zadržavati sukladno Direktivi uključuju podatke potrebne za pronalaženje i identifikaciju izvora i odredišta komunikacije, datuma, vremena i trajanja komunikacije, telefonskih brojeva s kojih se poziva i koje se poziva te IP adresa. Ti podaci, „uzeti zajedno, mogu omogućiti donošenje vrlo preciznih zaključaka o privatnom životu osoba čiji su podaci zadržani, kao što su svakodnevne navike, mjesta trajnih ili privremenih boravaka, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te osobe posjećivale”.

Stoga zadržavanje osobnih podataka na temelju Direktive čini posebno ozbiljno miješanje u prava na privatnost i zaštitu osobnih podataka. Međutim, SEU je smatrao da miješanje nije negativno utjecalo na suštinu tih prava. Kad je riječ o pravu na privatnost, njegova suština nije bila ugrožena jer Direktivom nije bilo dozvoljeno stjecanje saznanja o samom sadržaju elektroničkih komunikacija. Slično tome, suština prava na zaštitu osobnih podataka nije

63 Odluka SEU-a da Odluku Komisije 520/2000/EZ proglasi nevaljanom također se temeljila na drugim osnovama koje se razmatraju u drugim dijelovima priručnika. SEU je prvenstveno smatrao da se Odlukom nezakonito ograničavaju ovlasti nacionalnih nadzornih tijela za zaštitu podataka. Usto, u sustavu koji se temelji na načelu „sigurne luke” pojedincima nisu bili dostupni nikakvi pravni lijekovi ako su htjeli pristupiti osobnim podacima o sebi i/ili osigurati njihovo ispravljanje ili brisanje. Stoga je ugrožena i suština temeljnog prava na djelotvornu sudsku zaštitu, zajamčenog člankom 47. Povelje.

64 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [V], 8. travnja 2014.

bila ugrožena jer se Direktivom od pružatelja elektroničkih komunikacijskih usluga zahtijevalo da poštuju određena načela zaštite podataka i sigurnosti podataka te da u tu svrhu provedu odgovarajuće tehničke i organizacijske mjere.

Nužnost i proporcionalnost

Člankom 52. stavkom 1. Povelje propisuje se da su, podložno načelu proporcionalnosti, ograničenja ostvarivanja temeljnih prava i sloboda priznatih Poveljom dopustiva samo ako su nužna.

Ograničenje može biti **nužno** ako je potrebno donijeti mjere za ostvarenje cilja od javnog interesa, no nužnost, kako je tumači SEU, također podrazumijeva da done-sene mjere moraju biti manje nametljive u odnosu na druge mogućnosti ostvarivanja istog cilja. Za ograničenja prava na poštovanje privatnog života i zaštitu osobnih podataka SEU primjenjuje strogi „test nužnosti” smatrajući da se „izuzeća i ograničenja moraju primjenjivati samo ako su strogo nužna”. Ako se neko ograničenje smatra strogo nužnim, treba ocijeniti i je li proporcionalno.

Proporcionalnost znači da prednosti koje proizlaze iz ograničenja trebaju prevagnuti nad štetom koju ono uzrokuje ostvarivanju predmetnih temeljnih prava⁶⁵. Kako bi se umanjili nedostaci i rizici za ostvarivanje prava na privatnost i zaštitu podataka, važno je da ograničenja sadržavaju odgovarajuće zaštitne mjere.

Primjer: U predmetu *Volker und Markus Schecke*⁶⁶ SEU je zaključio da su nametanjem obveze objavljivanja osobnih podataka svih fizičkih osoba koje su bile korisnici potpore iz određenih poljoprivrednih fondova bez pravljenja razlike na temelju bitnih kriterija kao što su razdoblja tijekom kojih su te osobe primale potporu, učestalost ili narav i iznos potpore Vijeće i Komisija prekoračili ograničenja propisana načelom proporcionalnosti.

65 EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mjera), str. 5.

66 SEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010., t. 89. i 86.

Stoga je SEU zaključio da je određene odredbe Uredbe Vijeća (EZ) br. 1290/2005 nužno proglasiti nevaljanima, a Uredbu (EZ) br. 259/2008 proglasiti nevaljanom u cijelosti⁶⁷.

Primjer: U predmetu *Digital Rights Ireland*⁶⁸ SEU je zaključio da miješanjem u pravo na privatnost koje je uzrokovano primjenom Direktive o zadržavanju podataka nije ugrožena suština tog prava jer se Direktivom zabranjuje zadržavanje sadržaja elektroničkih komunikacija. Međutim, zaključio je i da Direktiva nije usklađena s člancima 7. i 8. Povelje te ju je proglasio nevaljanom. Budući da se podaci o prometu i lokaciji – kada se skupe i razmotre kao cjelina – mogu analizirati i pružaju detaljnu sliku privatnog života pojedinaca, to čini ozbiljno miješanje u ta prava. SEU je uzeo u obzir činjenicu da se Direktivom zahtijeva zadržavanje svih metapodataka o fiksnoj i mobilnoj telefoniji, pristupu internetu, internetskoj elektroničkoj pošti i internetskoj telefoniji, koji se primjenjuju na sva sredstva elektroničke komunikacije, čija je upotreba vrlo raširena u svakodnevnom životu. To je, zapravo, bilo miješanje koje je utjecalo na cijelu populaciju Europe. Kada se u obzir uzmu opseg i ozbiljnost takva miješanja, prema mišljenju SEU-a, zadržavanje podataka o prometu i lokaciji može se opravdati samo svrhom borbe protiv teških kaznenih djela. Usto, Direktivom nisu utvrđeni nikakvi objektivni kriteriji kojima bi se osiguralo da je pristup nadležnih nacionalnih tijela zadržanim podacima ograničen na ono što je strogo nužno. Direktiva također ne definira materijalne i postupkovne uvjete kojima se uređuje pristup nacionalnih tijela zadržanim podacima koji nisu podvrgnuti prethodnom preispitivanju suda ili drugog nezavisnog tijela te upotreba tih podataka.

SEU je do sličnog zaključka došao i u spojenim predmetima *Tele2 Sverige AB protiv Post- och telestyrelsen* i *Secretary of State for the Home Department protiv Toma Watsona i drugih*⁶⁹. Ti su se predmeti odnosili na zadržavanje podataka o prometu i lokaciji koji obuhvaćaju „sve pretplatnike i registrirane

67 Uredba Vijeća (EZ) br. 1290/2005 od 21. lipnja 2005. o financiranju zajedničke poljoprivredne politike, SL 2005 L 209; Uredba Komisije (EZ) br. 259/2008 od 18. ožujka 2008. o utvrđivanju detaljnih pravila za primjenu Uredbe Vijeća (EZ) br. 1290/2005 u pogledu objavljivanja informacija o korisnicima sredstava iz Europskog fonda za jamstva u poljoprivredi (EFJP) i Europskog poljoprivrednog fonda za ruralni razvoj (EPFRR), SL 2008 L 76.

68 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. travnja 2014., t. 39.

69 SEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i dr.* [VV], 21. prosinca 2016., t. 105. i 106.

korisnike te [...] sva sredstva elektroničke komunikacije” i metapodatke, pri čemu se ne predviđa „razlikovanje, ograničenje ili iznimku s obzirom na cilj koji se želi postići”⁷⁰. U ovom predmetu uvjet zadržavanja podataka o pojedincu nije bio je li on ili nije izravno ili neizravno povezan s teškim kaznenim djelima ni jesu li njegove komunikacije bile važne za nacionalnu sigurnost. Budući da je izostala nužna poveznica između zadržanih podataka i prijetnje javnoj sigurnosti, kao i ograničenje vremenskog razdoblja ili zemljopisnog područja, SEU je zaključio da nacionalno zakonodavstvo prelazi granice onoga što je strogo nužno za svrhu borbe protiv teških kaznenih djela⁷¹.

Sličan je pristup u pogledu nužnosti primijenio i Europski nadzornik za zaštitu podataka u svojem Paketu alata za određivanje nužnosti mjera⁷². Paket alata služi za procjenu sukladnosti predloženih mjera s pravom EU-a o zaštiti podataka. Paket je razvijen kako bi pomogao donositeljima politika i zakonodavcima u EU-u koji su zaduženi za pripremu ili preispitivanje mjera koje uključuju obradu osobnih podataka i kojima se ograničava pravo na zaštitu osobnih podataka te druga prava i slobode utvrđene u Povelji.

Ciljevi od općeg interesa

Da bi bilo opravdano, svako ograničenje ostvarivanja prava priznatih Poveljom mora u suštini ispunjavati ciljeve općeg interesa koje priznaje Unija ili potrebu za zaštitom prava i sloboda drugih. Kad je riječ o potrebi za zaštitom prava i sloboda drugih, pravo na zaštitu osobnih podataka često je povezano s drugim temeljnim pravima. U [dijelu 1.3.](#) prikazana je detaljna analiza tih poveznica. Ciljevi od općeg interesa uključuju opće ciljeve EU-a utvrđene u članku 3. Ugovora o Europskoj uniji (UEU), poput promicanja mira i dobrobiti njezinih naroda, socijalne pravde i zaštite, uspostavljanja područja slobode, sigurnosti i pravde na kojem je osigurano slobodno kretanje osoba zajedno s odgovarajućim mjerama u pogledu sprečavanja i suzbijanja kriminala te drugih ciljeva i interesa zaštićenih pojedinim odredbama ugovora⁷³. U tom se pogledu u Općoj uredbi o zaštiti podataka dodatno razrađuje članak 52. stavak 1. Povelje: u članku 23. stavku 1. Uredbe navodi se niz ciljeva od općeg interesa koji se smatraju legitimnima za ograničavanje prava pojedinaca, pod uvjetom

⁷⁰ *Ibid.*, t. 105.

⁷¹ *Ibid.*, t. 107.

⁷² EDPs (2017.), Paket alata za određivanje nužnosti mjera, Bruxelles, 11. travnja 2017.

⁷³ Objašnjenja koja se odnose na Povelju Europske unije o temeljnim pravima (2007/C 303/02), SL 2007 C 303, str. 17.–35.

da se takvim ograničenjem poštuje bit prava na zaštitu osobnih podataka te da je ono nužno i proporcionalno. Među navedenim su ciljevima od javnog interesa nacionalna sigurnost i obrana, sprečavanje kaznenih djela, zaštita važnih gospodarskih i financijskih interesa EU-a ili država članica, javno zdravstvo i socijalna sigurnost.

Važno je dovoljno detaljno definirati i objasniti cilj od općeg interesa koji se nastoji ostvariti ograničenjem jer će se nužnost ograničenja procijeniti s obzirom na taj element. Jasan i detaljan opis cilja ograničenja i predloženih mjera neophodan je za omogućivanje procjene njegove nužnosti⁷⁴. Cilj koji se nastoji ostvariti te nužnost i proporcionalnost ograničenja usko su povezani.

Primjer: Predmet *Schwarz protiv Stadt Bochum*⁷⁵ odnosio se na ograničenje prava na poštovanje privatnog života i prava na zaštitu osobnih podataka koje proizlazi iz uzimanja i pohranjivanja otisaka prstiju kada države članice izdaju putovnice⁷⁶. Tužitelj je podnio zahtjev za izradu putovnice Gradu Bochumu u Njemačkoj, no odbio je dati otiske prstiju. Nakon toga Grad Bochum odbio je njegov zahtjev za izradu putovnice. On je zatim pokrenuo postupak pred njemačkim sudom radi izdavanja putovnice bez davanja otisaka prstiju. Njemački sud uputio je predmet SEU-u, uz pitanje može li se članak 1. stavak 2. Uredbe (EZ) br. 2252/2004 o standardima za sigurnosna obilježja i biometrijske podatke u putovnicama i putnim ispravama koje izdaju države članice smatrati valjanim.

SEU je istaknuo da su otisci prstiju **osobni podaci** jer objektivno sadržavaju jedinstvene informacije o pojedincima koje omogućuju njihovu preciznu identifikaciju, a uzimanje i pohrana otisaka prstiju predstavljaju obradu. Takva obrada, regulirana člankom 1. stavkom 2. Uredbe (EZ) br. 2252/2004, prijetnja je pravima na poštovanje privatnog života i zaštitu osobnih podataka⁷⁷. Međutim, članak 52. stavak 1. Povelje omogućuje postavljanje ograničenja pri ostvarivanju tih prava pod uvjetom da su takva ograničenja zakonita, da poštuju suštinu tih prava te da su sukladno načelu proporcionalnosti nužna i da istinski ispunjavaju ciljeve od općeg interesa koje je prepoznala Unija, ili pak potrebu za zaštitom prava i sloboda drugih.

74 EDPS (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mjera), Bruxelles, 11. travnja 2017., str. 4.

75 SEU, C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. listopada 2013.

76 *Ibid.*, t. od 33. do 36.

77 *Ibid.*, t. od 27. do 30.

U ovom predmetu SEU je prvo istaknuo da se ograničenje koje proizlazi iz uzimanja i pohranjivanja otisaka prstiju prilikom izdavanja putovnica mora smatrati **zakonitim** jer su takvi postupci propisani člankom 1. stavkom 2. Uredbe (EZ) br. 2252/2004. Drugo, navedena Uredba osmišljena je kako bi se spriječilo krivotvorenje putovnica i njihova zloupotreba. Stoga članak 1. stavak 2., među ostalim, služi za sprečavanje nezakonitog ulaska u EU, čime se nastoji ispuniti cilj od općeg interesa koji priznaje Unija. Treće, na temelju dokaza koji su bili dostupni SEU-u nije bilo jasno niti se tvrdilo da se ograničenjima za ostvarivanje spomenutih prava u ovom predmetu nije poštovala suština tih prava. Četvrto, za pohranu otisaka prstiju na vrlo siguran medij za pohranu iz te odredbe potrebna je sofisticirana tehnologija. Takvom će se pohranom vjerojatno smanjiti opasnost od krivotvorenja putovnica i olakšati rad tijela nadležnih za provjeru autentičnosti putovnica na granicama EU-a. Činjenica da ta metoda nije potpuno pouzdana nije odlučujući čimbenik. Iako se njome ne sprečava svako prihvaćanje osoba koje nemaju odobrenje za to, dostatna je da se znatno smanji vjerojatnost njihova prihvaćanja. S obzirom na navedeno, SEU je zaključio da je uzimanje i pohranjivanje otisaka prstiju utvrđeno u članku 1. stavku 2. Uredbe (EZ) br. 2252/2004 bilo primjereno za ostvarenje ciljeva te Uredbe, a time i cilja sprečavanja nezakonitog ulaska u EU⁷⁸.

SEU je zatim ocijenio je li takva obrada **nužna**, primjećujući da je predmetni postupak uključivao uzimanje otisaka samo dvaju prstiju, koji su, štoviše, uglavnom vidljivi drugima, stoga nije riječ o postupku intimne prirode. Njime se također ne uzrokuje nikakva posebna fizička ili mentalna nelagoda osobi čiji se otisci uzimaju, svakako ništa veća nego snimanje fotografije lica te osobe. Također treba napomenuti da je jedina stvarna alternativa uzimanju otisaka prstiju u ovom postupku pred SEU-om bilo skeniranje šarenica oka. Ništa u spisu predmeta podnesenog SEU-u nije upućivalo na to da bi se potpunijim postupkom manje miješalo u prava priznata člancima 7. i 8. Povelje nego uzimanjem otisaka prstiju. Nadalje, u pogledu učinkovitosti tih dviju metoda, poznato je da tehnologija prepoznavanja šarenica još nije dovoljno napredna kao tehnologija prepoznavanja otisaka prstiju i trenutačno je znatno skuplja od postupka za usporedbu otisaka prstiju te je zbog toga manje prikladna za opću primjenu. U skladu s tim SEU nije bio upućen ni u kakve mjere koje bi

78 *Ibid.*, t. od 35. do 45.

istovremeno bile dovoljno učinkovite u ostvarenju cilja zaštite od zloupotrebe putovnica i predstavljale manju prijetnju pravima priznatima člancima 7. i 8. Povelje od mjera koje proizlaze iz metode upotrebe otisaka prstiju⁷⁹.

SEU je napomenuo da se u članku 4. stavku 3. Uredbe (EZ) br. 2252/2004 izričito navodi da se otisci prstiju mogu upotrijebiti samo za provjeru autentičnosti putovnice i identiteta njezina vlasnika, a u članku 1. stavku 2. Uredbe nije utvrđena pohrana otisaka prstiju, osim u samoj putovnici, koja pripada isključivo vlasniku. Stoga Uredba ne pruža pravnu osnovu za centraliziranu pohranu podataka prikupljenih na temelju nje ni za upotrebu takvih podataka u druge svrhe osim sprečavanja nezakonitog ulaska u EU⁸⁰. S obzirom na sve navedeno SEU je zaključio da razmatranjem pitanja koje mu je upućeno nije otkriveno ništa što bi moglo utjecati na valjanost članka 1. stavka 2. Uredbe (EZ) br. 2252/2004.

Odnos između Povelje i Europske konvencije o ljudskim pravima (EKLJP)

Unatoč različitom tekstu, uvjeti za zakonita ograničenja prava iz članka 52. stavka 1. Povelje podsjećaju na članak 8. stavak 2. EKLJP-a u pogledu poštovanja privatnog života. U svojim sudskim praksama SEU i ESLJP često međusobno upućuju na presude koje donose, što je dio neprekidnog dijaloga između tih dvaju sudova, kako bi se postiglo usklađeno tumačenje propisa o zaštiti podataka. U članku 52. stavku 3. Povelje navodi se: „U onoj mjeri u kojoj ova Povelja sadržava prava koja odgovaraju pravima zajamčenima Konvencijom za zaštitu ljudskih prava i temeljnih sloboda, značenje i opseg primjene tih prava jednaki su onima iz spomenute Konvencije.” Međutim, članak 8. Povelje ne odgovara posve nijednom članku iz EKLJP-a⁸¹. Članak 52. stavak 3. Povelje odnosi se na sadržaj i opseg primjene prava zaštićenih pojedinim pravnim poretkom, a ne na uvjete njihova ograničenja. Međutim, s obzirom na širi kontekst dijaloga i suradnje između dvaju sudova, SEU u svojim analizama može uzeti u obzir kriterije za zakonito ograničenje na temelju članka 8. EKLJP-a, sukladno tumačenju ESLJP-a. Moguć je i alternativni scenarij u kojemu ESLJP može upućivati na uvjete za zakonito ograničenje na temelju Povelje. U svakom slučaju, potrebno je uzeti u obzir i da u EKLJP-u ne postoji članak jednakovrijedan članku 8. Povelje koji bi se odnosio na zaštitu osobnih podataka, a posebno na prava

79 SEU, C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. listopada 2013., t. od 46. do 53.

80 *Ibid.*, t. od 56. do 61.

81 EDPS (2017.), *Necessity Toolkit*, Bruxelles, 11. travnja 2017., str. 6.

ispitanika, legitimnu osnovu obrade podataka i nadzor neovisnog tijela. Određeni elementi članka 8. Povelje mogu se pronaći u sudskoj praksi ESJLP-a, razvijenoj na temelju članka 8. EKJLP-a i povezanoj s Konvencijom br. 108⁸². Tom se poveznicom osigurava da SEU i ESJLP utječu jedan na drugoga u pitanjima povezanim sa zaštitom podataka.

1.3. Odnos s drugim pravima i legitimnim interesima

Ključne točke

- Pravo na zaštitu podataka obično je povezano s drugim pravima kao što su sloboda izražavanja i pravo na primanje i širenje informacija.
- Taj je odnos često ambivalentan: u nekim je slučajevima pravo na zaštitu osobnih podataka u sukobu s određenim pravom, no postoje i slučajevi u kojima se pravom na zaštitu osobnih podataka zapravo osigurava poštovanje tog istog drugog prava. Takav je slučaj primjerice sa slobodom izražavanja s obzirom na to da je čuvanje poslovne tajne element prava na poštovanje privatnog života.
- Potreba za zaštitom prava i sloboda drugih jedan je od kriterija prema kojima se procjenjuje zakonito ograničenje prava na zaštitu osobnih podataka.
- Kada su različita prava dovedena u pitanje, sudovi moraju odvagnuti interese kako bi ih uskladili.
- Općom uredbom o zaštiti podataka propisuje se da države članice usklade pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja.
- Države članice mogu također donijeti određene propise u nacionalnim zakonodavstvima kako bi uskladile pravo na zaštitu osobnih podataka s javnim pristupom službenim dokumentima i obvezama čuvanja poslovne tajne.

Pravo na zaštitu osobnih podataka nije apsolutno pravo. Uvjeti za zakonito ograničenje tog prava detaljno su objašnjeni u prethodnom dijelu. Jedan od kriterija za zakonito ograničenje prava, priznat i pravom Vijeća Europe i EU-a, jest nužnost miješanja u zaštitu podataka radi zaštite prava i sloboda drugih osoba. Kada se zaštita podataka povezuje s drugim pravima, i ESJLP i SEU opetovano su tvrdili da je potrebno

82 Objašnjenja koja se odnose na Povelju Europske unije o temeljnim pravima (2007/C 303/02), čl. 8.

odvagati interese kada se primjenjuju i tumače članak 8. EKLJP-a i članak 8. Povelje⁸³. U nekoliko važnih primjera opisano je kako postupak odvagivanja izgleda.

Uz postupak odvagivanja interesa koji provode ovi sudovi, pojedine države mogu po potrebi donijeti zakonodavstvo kojim bi se pravo na zaštitu osobnih podataka usklađilo s drugim pravima. Zbog toga Opća uredba o zaštiti podataka omogućuje donošenje niza nacionalnih izuzeća.

Kad je riječ o slobodi izražavanja, OUZP-om se državama članicama propisuje da zakonom usklađuju „pravo na zaštitu osobnih podataka u skladu s ovom Uredbom s pravom na slobodu izražavanja i informiranja, što uključuje obradu u novinarske svrhe i svrhe akademskog, umjetničkog ili književnog izražavanja”⁸⁴. Države članice također mogu donijeti zakone za usklađivanje zaštite podataka s javnim pristupom službenim dokumentima i obvezama čuvanja profesionalne tajne kao jednog od oblika poštovanja privatnog života⁸⁵.

1.3.1. Sloboda izražavanja

Jedno od prava koje se najviše povezuje s pravom na zaštitu podataka jest pravo na slobodu izražavanja.

Sloboda izražavanja zaštićena je člankom 11. Povelje („Sloboda izražavanja i informiranja”). To pravo obuhvaća „slobodu mišljenja te primanja i davanja informacija i ideja bez miješanja tijela vlasti i bez obzira na granice”. Sukladno članku 11. Povelje i članku 10. EKLJP-a, slobodom informiranja štiti se pravo ne samo na davanje već i na primanje informacija.

Ograničenja slobode izražavanja moraju ispunjavati prethodno opisane kriterije utvrđene u članku 52. stavku 1. Povelje. Osim toga, članak 11. odgovara članku 10. EKLJP-a. Sukladno članku 52. stavku 3. Povelje, u mjeri u kojoj ona sadržava prava koja odgovaraju pravima zajamčenima EKLJP-om, „značenje i opseg primjene tih prava jednaki su onima iz spomenute Konvencije”. Ograničenja koja se zakonito

83 ESLJP, *Von Hannover protiv Njemačke* (br. 2) [VV], br. 40660/08 i 60641/08, 7. veljače 2012.; SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. studenoga 2011., t. 48.; SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. siječnja 2008., t. 68.

84 Opća uredba o zaštiti podataka, članak 85.

85 *Ibid.*, članci 86. i 90.

moгу nametnuti pravu zajamčenom u članku 11. Povelje stoga ne smiju premašiti ona iz članka 10. stavka 2. EKLJP-a. Drugim riječima, moraju biti zakonom propisana i nužna u demokratskom društvu „radi zaštite [...] ugleda ili prava drugih“. Takva prava obuhvaćaju prvenstveno pravo na poštovanje privatnog života i pravo na zaštitu osobnih podataka.

Odnos između zaštite osobnih podataka i slobode izražavanja reguliran je članom 85. Opće uredbe o zaštiti podataka naslovljenim „Obrada i sloboda izražavanja i informiranja“. Prema tom članku, države članice zakonom usklađuju pravo na zaštitu osobnih podataka s pravom na slobodu izražavanja i informiranja. Konkretno, izuzeća i odstupanja od određenih poglavlja Opće uredbe o zaštiti podataka uvode se u novinarske svrhe i svrhe akademskog, umjetničkog ili književnog izražavanja ako su ona potrebna kako bi se uskladilo pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja.

Primjer: U predmetu *Tietosuoja-valtuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy*⁸⁶ od SEU-a je zatraženo da definira odnos između zaštite podataka i slobode tiska⁸⁷. Sud je morao ispitati slučaj objave poreznih podataka otprilike 1,2 milijuna fizičkih osoba putem SMS poruka, pri čemu je podatke spomenuto društvo zakonito dobilo od finskih poreznih tijela. Finsko nadzorno tijelo za zaštitu podataka izdalo je odluku kojom se od društva traži da prestane objavljivati te podatke. Društvo je osporilo tu odluku na nacionalnom sudu, koji je zatražio obrazloženje SEU-a o tumačenju Direktive o zaštiti podataka. SEU je prvenstveno trebao provjeriti treba li se obrada osobnih podataka, koje su porezna tijela stavila na raspolaganje kako bi se korisnicima mobilnih telefona omogućilo primanje poreznih podataka drugih fizičkih osoba, smatrati djelatnošću koja se provodi isključivo u novinarske svrhe. Zaključivši da su se djelatnosti društva sastojale od „obrade osobnih podataka“ u smislu članka 3. stavka 1. Direktive o zaštiti podataka, SEU je analizirao članak 9. Direktive (o obradi osobnih podataka i slobodi izražavanja). Najprije se osvrnuo na važnost prava na slobodu izražavanja u svakom demokratskom društvu, držeći da se pojmovi povezani s tom slobodom,

86 SEU, C-73/07, *Tietosuoja-valtuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy* [WV], 16. prosinca 2008., t. 56., 61. i 62.

87 Predmet se odnosio na tumačenje članka 9. Direktive o zaštiti podataka, sada zamijenjenog člankom 85. Opće uredbe o zaštiti podataka, u kojemu stoji sljedeće: „Države članice utvrđuju iznimke ili odstupanja od odredbi ovog poglavlja, poglavlja IV. i poglavlja VI. za obradu osobnih podataka izvršenih isključivo u novinarske svrhe ili radi umjetničkog ili književnog izražavanja jedino ako su potrebni radi usklađivanja prava na privatnost s propisima o slobodi izražavanja.“

poput novinarstva, trebaju široko tumačiti. Zatim je napomenuo da se radi postizanja ravnoteže između dvaju temeljnih prava, izuzeća i ograničenja prava na zaštitu podataka moraju primjenjivati samo ako je to strogo nužno. U tim je okolnostima SEU smatrao da se djelatnosti kao što su one koje su provodila ta dva društva, a koje su se ticale podataka iz dokumenata u javnoj domeni u okviru nacionalnog zakonodavstva, mogu klasificirati kao „novinarske djelatnosti” ako je njihov predmet otkrivanje informacija, mišljenja i ideja javnosti, neovisno o mediju iskorištenom za njihov prijenos. Također je presudio da takve djelatnosti nisu ograničene na medijska društva i da se mogu obavljati u svrhe stjecanja profita. Međutim, SEU je prepustio nacionalnom sudu odluku o tome je li tako bilo u ovom konkretnom slučaju.

Isti je predmet preispitao i ESLJP, nakon što je na temelju smjernica SEU-a nacionalni sud odlučio da je nalog nadzornog tijela da se obustavi objava svih poreznih podataka opravdano miješanje u slobodu izražavanja društva. ESLJP je podržao takav pristup⁸⁸. Zaključio je da je unatoč miješanju u pravo društva na širenje informacija to miješanje bilo u skladu sa zakonom, njime se nastojao ostvariti legitiman cilj te je bilo nužno u demokratskom društvu.

Sud je podsjetio na kriterije iz sudske prakse kojima bi se nacionalna tijela trebala voditi, kao i sam ESLJP, prilikom odvagivanja slobode izražavanja i prava na poštovanje privatnog života. Kada su u pitanju politički govor ili debata o nekom pitanju od javnog interesa, malo je prostora za ograničenje prava na primanje i širenje informacija jer javnost ima pravo na informiranje, „a to je osnovno pravo u demokratskom društvu”⁸⁹. Međutim, ne može se smatrati da novinski članci kojima je cilj isključivo utažiti znatiželju određenih čitatelja za pojedinostima iz privatnog života neke osobe pridonose raspravi od javnog interesa. Izuzeća od propisa zaštite podataka za novinske svrhe predviđena su da novinarima omoguće pristup podacima te njihovo prikupljanje i obradu kako bi mogli obavljati svoje novinarske poslove. Stoga je doista postojao javni interes za pružanje pristupa velikim količinama poreznih podataka i omogućivanje njihova prikupljanja i obrade društvima tužiteljima. S druge strane, ESLJP je zaključio da nije bilo javnog interesa u skupnoj objavi takvih neobrađenih podataka u novinama, u neizmijenjenom obliku i bez ikakvih analitičkih radnji. Informacije o oporezivanju mogle su znatiželjnim građanima

88 ESLJP, *Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske* [VV], br. 931/13, 27. lipnja 2017.

89 *Ibid.*, t. 169.

omogućiti kategoriziranje pojedinaca prema njihovu ekonomskom statusu te utajiti znatiželju javnosti za informacijama o privatnim životima drugih osoba. To se nije moglo smatrati doprinosom raspravi od javnog interesa.

Primjer: U predmetu *Google Spain*⁹⁰ SEU je razmatrao je li društvo Google bilo obvezano izbrisati zastarjele informacije o tužiteljevim financijskim poteškoćama iz popisa rezultata pretraživanja. Kada se tužiteljevo ime tražilo u internetskoj tražilici Google, rezultati pretrage uključivali su poveznice na stare novinske članke u kojima se navodila njegova povezanost sa stečajnim postupkom. Tužitelj je to smatrao kršenjem svojih prava na poštovanje privatnog života i zaštitu osobnih podataka s obzirom na to da je postupak dovršen godinama ranije, pa su takve reference bile nevažne.

SEU je prvo pojasnio da internetske tražilice i rezultati pretraživanja koji sadržavaju osobne podatke mogu poslužiti za izradu detaljnog profila osobe. S obzirom na to da društvo postaje sve više digitalizirano, zahtjev da osobni podaci budu točni i da njihova objava ne prelazi ono što je nužno, odnosno pružanje informacija javnosti, ključan je za osiguravanje visoke razine zaštite podataka pojedinaca. „[V]oditelj obrade u okviru svojih odgovornosti, nadležnosti i mogućnosti [mora] osigurati da ta aktivnost zadovoljava uvjete” iz prava Unije kako bi predviđena jamstva mogla razviti svoj puni učinak. To znači da pravo na brisanje osobnih podataka kada njihova obrada više nije potrebna ili su oni zastarjeli također obuhvaća internetske tražilice, koje se smatraju i voditeljima obrade, a ne samo izvršiteljima obrade (vidjeti dio 2.3.1.).

Prilikom razmatranja je li Google obvezan ukloniti poveznice povezane s tužiteljem, SEU je zaključio da u određenim uvjetima pojedinci imaju pravo na brisanje svojih osobnih podataka iz rezultata pretraživanja internetske tražilice. Na to se pravo može pozvati kada informacije o nekom pojedincu nisu točne, dostatne ili relevantne ili ih je previše za svrhu obrade podataka. SEU je potvrdio da to pravo nije apsolutno, nego se mora odvagati u odnosu na druga prava, posebice u odnosu na interes i pravo šire javnosti na pristup tim informacijama. Za svaki zahtjev za brisanjem potrebna je pojedinačna procjena kako bi se uspostavila ravnoteža između temeljnih prava na zaštitu osobnih podataka i privatni život ispitanika s jedne strane

90 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. od 81. do 83.

te legitimnih interesa svih korisnika interneta s druge. SEU je pružio smjernice o čimbenicima koje je potrebno uzeti u obzir prilikom odvagivanja interesa. Priroda tih informacija posebno je važan čimbenik. Ako su informacije osjetljive s obzirom na privatni život pojedinca te ne postoji javni interes za dostupnošću tih informacija, zaštita podataka i privatnost bile bi važnije od prava šire javnosti na pristup informacijama. S druge strane, ako je ispitanik javna ličnost ili su informacije takve da opravdavaju omogućivanje pristupa šire javnosti tim informacijama, tada je miješanje u temeljna prava na zaštitu podataka i privatnost opravdano.

Slijedom te presude, Radna skupina iz članka 29. usvojila je smjernice o provedbi odluke SEU-a. Smjernice sadržavaju popis uobičajenih kriterija koje nadzorna tijela primjenjuju prilikom obrade pritužbi povezanih sa zahtjevima pojedinaca za brisanjem te kojih bi se ta tijela trebala pridržavati prilikom odvagivanja prava⁹¹.

U pogledu usuglašavanja prava na zaštitu podataka i prava na slobodu izražavanja, Europski sud za ljudska prava donio je nekoliko orijentacijskih presuda.

Primjer: U predmetu *Axel Springer AG protiv Njemačke*⁹² ESLJP je smatrao da je zabranom kojom se društvu tužitelju onemogućilo objavljivanje članka o uhićenju i osudi poznatog glumca prekršen članak 10. EKLJP-a. ESLJP se ponovno pozvao na kriterije koje je utvrdio u svojoj sudskoj praksi i koje treba uzeti u obzir prilikom odvagivanja prava na slobodu izražavanja i prava na poštovanje privatnog života:

- je li događaj na koji se odnosio objavljeni članak bio od općeg interesa,
- je li dotična osoba javna ličnost, te
- kako su informacije dobivene i jesu li bile pouzdane.

⁹¹ Radna skupina iz članka 29. (2014.), *Guidelines on the implementation of the CJEU judgment on „Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12* (Smjernice o provedbi presude Suda Europske unije u predmetu „Google Spain i Inc protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje Gonzáleza” C-131/12), WP 225, Bruxelles, 26. studenoga 2014.

⁹² ESLJP, *Axel Springer AG protiv Njemačke* [VV], br. 39954/08, 7. veljače 2012., t. 90. i 91.

ESLJP je utvrdio da su uhićenje i osuda glumca javna pravosudna činjenica te da su stoga od javnog interesa, da je glumac dovoljno poznat da bi se smatrao javnom ličnosti te da su informacije dobivene iz ureda javnog tužitelja, pa stranke nisu osporavale njihovu točnost. Stoga ograničenja objave nametnuta društvu nisu bila opravdano proporcionalna legitimnom cilju zaštite privatnog života tužitelja. ESLJP je stoga zaključio da je došlo do kršenja članka 10. Konvencije.

Primjer: Predmet *Coudec i Hachette Filipacchi Associés protiv Francuske*⁹³ odnosio se na objavu intervjua s gđom Coste u francuskom tjedniku u kojemu je ona izjavila da je knez Albert od Monaka otac njezina sina. U intervjuu je također opisan odnos gđe Coste s knezom i način na koji je on reagirao na rođenje djeteta, uz fotografije kneza s djetetom. Knez Albert pokrenuo je sudski postupak protiv izdavačkog društva zbog kršenja njegova prava na zaštitu privatnog života. Francuski sudovi ustvrdili su da je objava članka uzrokovala nepovratnu štetu knezu Albertu te su naložili nakladniku da plati odštetu i objavi pojedinosti presude na naslovnici časopisa.

Nakladnici časopisa pokrenuli su postupak pred ESLJP-om, tvrdeći da su se francuski sudovi neopravdano umiješali u njihovo pravo na slobodu izražavanja. ESLJP je trebao odvagnuti pravo kneza Alberta na poštovanje privatnog života s pravom nakladnika na izražavanje te pravom šire javnosti na informacije. Pravo gđe Coste da podijeli svoju priču s javnosti i interes djeteta za službeno utvrđivanje odnosa oca i djeteta također su bili važni čimbenici.

ESLJP je smatrao da objava intervjua predstavlja miješanje u privatni život kneza te je preispitao je li miješanje bilo nužno. Ustvrdio je da se objava odnosila na javnu ličnost i pitanje od javnog interesa. Budući da su građani Monaka imali interes za saznanje o postojanju kneževa djeteta jer je budućnost nasljedne monarhije „neodvojivo povezana s postojanjem potomaka“, to je pitanje od interesa za javnost⁹⁴. Sud je također istaknuo da je članak omogućio gđi Coste i njezinu djetetu ostvarivanje prava na slobodu izražavanja. Nacionalni sudovi nisu propisno uzeli u obzir načela i kriterije razvijene u sklopu sudske prakse ESLJP-a za odvagivanje prava na poštovanje privatnog života i prava na slobodu izražavanja. Naposljetku je zaključio da je Francuska prekršila članak 10. EKLJP-a po pitanju slobode izražavanja.

93 ESLJP, *Coudec i Hachette Filipacchi Associés protiv Francuske* [VV], br. 40454/07, 10. studenoga 2015.

94 *Ibid.*, t. od 104. do 116.

U sudskoj praksi ESLJP-a jedan je od ključnih kriterija koji se tiču odvagivanja tih prava kriterij doprinosa koji dotično izražavanje daje raspravi od općeg javnog interesa.

Primjer: U predmetu *Mosley protiv Ujedinjene Kraljevine*⁹⁵ nacionalni je tjednik objavio intimne fotografije tužitelja, poznate osobe koja je naknadno pokrenula građansku parnicu protiv nakladnika te joj je dodijeljena odšteta. Unatoč ostvarenoj novčanoj naknadi tužitelj je podnio pritužbu u kojoj je naveo da je i dalje žrtva kršenja prava na privatnost jer mu je uskraćena mogućnost da ishodi sudsku zabranu prije objave predmetnih fotografija s obzirom na to da ne postoji nikakav zakonski uvjet prema kojemu bi novine morale obavijestiti osobu prije objave.

ESLJP je naveo da iako je navedeni materijal objavljen više u zabavne nego u obrazovne svrhe, nedvojbeno se podrazumijevala zaštita zajamčena člankom 10. EKLJP-a te se takva objava mogla nadovezati na zahtjeve iz članka 8. EKLJP-a s obzirom na to da su informacije bile privatne i intimne naravi te nije bilo javnog interesa za njihovu objavu. Ovdje je ipak valjalo obratiti posebnu pažnju pri ispitivanju ograničenja koja se mogu smatrati oblikom cenzure prije objave. Zbog neugodnosti koje bi moglo prouzročiti postavljanje zahtjeva za prethodnim obavješćivanjem, kao i zbog dvojbi o njegovoj učinkovitosti i velikog raspona procjena koje bi se njime otvorile u ovome području, ESLJP je zaključio da se člankom 8. ne zahtijeva pravno obvezujući zahtjev prethodnog obavješćivanja. U skladu s tim ESLJP je zaključio da nije prekršen članak 8.

Primjer: U predmetu *Bohlen protiv Njemačke*⁹⁶ tužitelj, poznati pjevač i glazbeni producent, objavio je autobiografiju iz koje je naknadno morao ukloniti određene odlomke na temelju sudske presude. Priča je dobila mnogo medijske pažnje u državi, a jedno je društvo za proizvodnju duhanskih proizvoda pokrenulo humorističnu marketinšku kampanju s referencama na ovaj događaj, u kojoj je upotrijebljeno ime tužitelja bez njegove privole. Tužitelj je neuspješno zahtijevao odštetu od marketinškog društva navodeći kršenje svojih prava na temelju članka 8. EKLJP-a. ESLJP se pozvao na kriterije na kojima se temelji odvagivanje prava na poštovanje privatnog života i prava na slobodu izražavanja te je zaključio da nije došlo do kršenja članka 8. Tužitelj je bio javna osoba i u oglasu nisu spomenute pojedinosti iz njegova privatnog

95 ESLJP, *Mosley protiv Ujedinjene Kraljevine*, br. 48009/08, 10. svibnja 2011., t. 129. i 130.

96 ESLJP, *Bohlen protiv Njemačke*, br. 53495/09, 19. veljače 2015., t. od 45. do 60.

života, nego javno poznat događaj koji je već bio medijski popraćen i koji je činio dio javne rasprave. Usto, oglas je bio humoristične naravi i nije sadržavao ništa ponižavajuće ili negativno u vezi s tužiteljem.

Primjer: U predmetu *Biriuk protiv Litve*⁹⁷ tužiteljica je pred ESLJP-om iznijela argument da Litva nije ispunila svoju obvezu osiguravanja poštovanja njezina prava na privatni život jer su joj, unatoč tome što su poznate dnevne novine ozbiljno povrijedile njezinu privatnost, nadležni nacionalni sudovi koji su ispitivali predmet dodijelili zanemarljivu novčanu odštetu. Prilikom dodjele naknade za prouzrokovanu nenovčanu štetu nacionalni su sudovi primijenili odredbe nacionalnog zakonodavstva koje se odnose na pružanje informacija javnosti, čime je nametnuta niska gornja granica naknade za nenovčanu štetu uzrokovanu nezakonitom objavom informacija o privatnom životu pojedinca u medijima. Predmet je pokrenut zbog objave članka na naslovnici najvećih dnevnih novina u Litvi u kojemu je pisalo da je tužiteljica HIV pozitivna. U članku je također iznesena kritika ponašanja tužiteljice i dovedene su u pitanje njezine moralne vrijednosti.

ESLJP je podsjetio da je zaštita osobnih podataka, a posebice medicinskih, od ključne važnosti za pravo na poštovanje privatnog života u okviru EKLJP-a. Povjerljivost zdravstvenih podataka posebno je važna s obzirom na to da otkrivanje medicinskih podataka (u ovom slučaju HIV status tužiteljice) može znatno utjecati na privatni i obiteljski život osobe, njezino zaposlenje i društvenu uključenost. Sud je posebnu važnost pridao činjenici da je, prema novinskom članku, medicinsko osoblje bolnice objavilo informacije o HIV statusu tužiteljice i tako jasno prekršilo svoju obvezu čuvanja liječničke tajne. Stoga nije bilo legitimnog miješanja u pravo na privatni život tužiteljice.

Članak su objavile novine, a sloboda izražavanja također je temeljno pravo prema EKLJP-u. Međutim, prilikom ispitivanja je li postojanje javnog interesa opravdavalo objavu te vrste podataka o tužiteljici, ESLJP je zaključio da je glavna svrha njihove objave bilo povećanje prodaje novina poticanjem znatiželje čitatelja. Za takvu se svrhu ne može smatrati da doprinosi raspravi od općeg interesa za društvo. Budući da je ovdje bilo riječ o „nečuvenoj zlouporabi slobode tiska“, znatna ograničenja u nadoknadi štete i nizak iznos naknade za prouzrokovanu nenovčanu štetu koja je osigurana nacionalnim

97 ESLJP, *Biriuk protiv Litve*, br. 23373/03, 25. studenoga 2008.

zakonodavstvom značili su da Litva nije ispunila svoju pozitivnu obvezu zaštite prava tužiteljice na privatni život. ESLJP je zaključio da je došlo do kršenja članka 8. EKLJP-a.

Pravo na slobodu izražavanja i pravo na zaštitu osobnih podataka nisu uvijek u sukobu. Postoje slučajevi u kojima se učinkovitom zaštitom osobnih podataka jamči sloboda izražavanja.

Primjer: SEU je u predmetu *Tele2 Sverige* utvrdio da je miješanje u temeljna prava utvrđena u člancima 7. i 8. Povelje, uzrokovano Direktivom 2006/24/EZ (Direktiva o zadržavanju podataka), bilo „široko i treba se smatrati osobito teškim. Nadalje, okolnost da se zadržavanje i naknadno korištenje podataka izvršava bez obavješćavanja pretplatnika ili registriranoga korisnika može kod dotičnih osoba [...] stvoriti osjećaj da je njihov privatni život predmet trajnog nadzora”. SEU je također zaključio da je opće zadržavanje podataka o prometu i lokaciji moglo utjecati na korisničku upotrebu elektroničke komunikacije i „stoga na uživanje njihove slobode izražavanja zajamčene u članku 11. Povelje”⁹⁸. U tom smislu, zahtijevanjem da se stroge zaštitne mjere za zadržavanje podataka ne provode na općenit način propisi za zaštitu podataka doprinose uživanju slobode izražavanja.

Kad je riječ o pravu na primanje informacija, koje je dio slobode izražavanja, sve je jača spoznaja o važnosti transparentnosti vlasti za funkcioniranje demokratskog društva. Transparentnost je cilj od općeg interesa kojim bi se stoga moglo opravdati miješanje u pravo na zaštitu podataka ako je to potrebno i proporcionalno, kao što je objašnjeno u [dijelu 1.2](#). U skladu s tim, u posljednja je dva desetljeća pravo pristupa dokumentima javnih tijela potvrđeno kao važno pravo svakog građanina EU-a te svake fizičke osobe koja prebiva odnosno pravne osobe sa sjedištem u nekoj državi članici.

98 SEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i dr.* [VV], 21. prosinca 2016., t. 37. i 101.; SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014., t. 28.

U okviru prava Vijeća Europe može se upućivati na načela sadržana u Preporuci o pristupu službenim dokumentima, koja je nadahnula autore Konvencije o pristupu službenim dokumentima (Konvencija br. 205)⁹⁹.

U okviru prava Unije pravo na pristup dokumentima zajamčeno je Uredbom (EZ) br. 1049/2001 o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (Uredba o pristupu dokumentima)¹⁰⁰. Člankom 42. Povelje i člankom 15. stavkom 3. Ugovora u funkcioniranju Europske unije to je pravo na pristup prošireno na pristup „dokumentima institucija, tijela, ureda i agencija Unije neovisno o njihovu mediju“.

To pravo može biti u suprotnosti s pravom na zaštitu podataka ako se pristupom dokumentu otkrivaju osobni podaci pojedinca. Člankom 86. Opće uredbe o zaštiti podataka jasno se utvrđuje da tijela javne vlasti i druga tijela mogu otkriti osobne podatke iz službenih dokumenata koje posjeduju u skladu s pravom Unije¹⁰¹ ili pravom države članice kako bi se javni pristup službenim dokumentima uskladio s pravom na zaštitu osobnih podataka u skladu s Uredbom.

Stoga može biti potrebno uravnotežiti zahtjeve za pristup dokumentima ili informacijama javnih tijela s pravom na zaštitu podataka osoba čiji su podaci sadržani u zatraženim dokumentima.

Primjer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*¹⁰² SEU je morao prosuditi proporcionalnost objave imena korisnika poljoprivrednih subvencija Europske unije te iznosa koje je svaki od njih primio, kako nalaže zakonodavstvo EU-a. Objavljivanjem takvih informacija nastojalo se povećati transparentnost i pridonijeti javnoj kontroli administracije u pogledu odgovarajuće uporabe javnih sredstava. Nekoliko je korisnika osporilo proporcionalnost takve objave.

99 Vijeće Europe, Odbor ministara (2002.), Preporuka R (81) 19 i Preporuka Rec(2002)2 državama članicama o pristupu službenim dokumentima, 21. veljače 2002.; Vijeće Europe, Konvencija o pristupu službenim dokumentima, CETS br. 205, 18. lipnja 2009. Konvencija još nije stupila na snagu.

100 Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije, SL 2001 L 145.

101 Članak 42. Povelje, članak 15. stavak 3. UFEU-a i Uredbe br. 1049/2009.

102 SEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010., t. od 47. do 52., 58., 66., 67., 75., 86. i 92.

Napominjući da pravo na zaštitu podataka nije apsolutno pravo, SEU je smatrao da je objava podataka o imenima korisnika dvaju poljoprivrednih fondova Unije s ukupnim iznosima primljenih potpora na internetskoj stranici zadiranje u privatni život korisnika, a osobito u zaštitu njihovih osobnih podataka.

SEU je smatrao da je takvo zadiranje u članke 7. i 8. Povelje omogućeno zakonom te da je njime ispunjen cilj od općeg interesa koji EU priznaje, tj. transparentnije korištenje fondovima zajednice. Unatoč tome, SEU je smatrao da je objava imena fizičkih osoba korisnika poljoprivredne potpore EU-a iz spomenutih dvaju fondova te ukupnih iznosa koje su primili neproporcionalna i neopravdana mjera uzimajući u obzir članak 52. stavak 1. Povelje. Naglasio je važnost obavješćivanja poreznih obveznika o uporabi javnih sredstava u demokratskom društvu. Međutim, s obzirom na to da „nije moguće općenito priznati nikakav automatski prioritet cilja transparentnosti nad pravom zaštite osobnih podataka”¹⁰³, institucije EU-a morale su odvagnuti interese transparentnosti Unije s ograničenjem ostvarivanja prava na privatnost i zaštitu podataka koje su korisnici doživjeli zbog objave.

SEU je smatrao da institucije EU-a nisu pravilno odvagnule te interese jer je bilo moguće zamisliti mjere koje bi manje štetno utjecale na temeljna prava pojedinaca, a istodobno učinkovito pridonijele cilju transparentnosti koji se nastojao ostvariti objavom. Na primjer, umjesto opće objave koja se odnosi na sve korisnike, s njihovim imenom i točnim iznosima koje je svaki od njih primio, mogla se učiniti razlika na temelju relevantnih kriterija kao što su razdoblja u kojima su te osobe primile potporu, učestalost potpore ili njezini iznosi i obilježja¹⁰⁴. Sud je stoga zakonodavstvo Europske unije o objavi informacija o korisnicima europskih poljoprivrednih fondova proglasio djelomično nevaljanim.

Primjer: U predmetu *Rechnungshof protiv Österreichischer Rundfunk i dr.*¹⁰⁵ SEU je preispitao usklađenost određenih austrijskih zakona sa zakonodavstvom EU-a o zaštiti podataka. Zakonom je bilo propisano da državno tijelo

¹⁰³ *Ibid.*, t. 85.

¹⁰⁴ *Ibid.*, t. 89.

¹⁰⁵ SEU, spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauermann protiv Österreichischer Rundfunk*, 20. svibnja 2003.

prikuplja i šalje podatke o prihodu u svrhu objave imena i prihoda zaposlenika raznih javnih tijela u okviru godišnjeg izvješća dostupnog široj javnosti. Neke su osobe odbile pružiti svoje podatke pozivajući se na zaštitu podataka.

SEU se u svojem mišljenju oslonio na zaštitu temeljnih prava kao općeg načela prava Unije i na članak 8. EKLJP-a, napominjući da Povelja u tom trenutku nije bila obvezujuća. Smatrao je da prikupljanje podataka o prihodu od rada pojedinca, a posebice njihovo prenošenje trećim stranama, pripada u područje primjene prava na poštovanje privatnog života i predstavlja kršenje tog prava. Miješanje se moglo opravdati ako je bilo u skladu sa zakonom, ako se njime nastojao ostvariti legitiman cilj te ako je bilo nužno u demokratskom društvu radi ostvarenja tog cilja. SEU je istaknuo da se austrijskim zakonom nastojao ostvariti legitiman cilj jer je taj cilj bio održavanje plaća javnih službenika unutar razumnih ograničenja, što je povezano s gospodarskom dobrobiti države. Međutim, interes Austrije u osiguravanju optimalnog iskorištavanja javnih sredstava morao se usporediti s ozbiljnošću miješanja u pravo dotičnih osoba na poštovanje njihova privatnog života.

Iako je SEU prepustio nacionalnom sudu da utvrdi je li objava podataka o prihodu pojedinaca bila nužna i proporcionalna cilju koji se nastojao ostvariti zakonom, pozvao je nacionalni sud da razmotri je li se takav cilj mogao ostvariti jednako učinkovito na manje invazivan način. Jedan je primjer toga prijenos osobnih podataka samo nadzornim javnim tijelima, a ne široj javnosti.

U kasnijim predmetima postalo je jasno da odvagivanje između zaštite podataka i pristupa dokumentima zahtijeva podrobnu analizu pojedinih slučajeva. Nijedno pravo ne može automatski poništiti drugo. SEU je u dvama predmetima imao priliku tumačiti pravo na pristup dokumentima koji sadržavaju osobne podatke.

Primjer: U predmetu *Europska komisija protiv Bavarian Lager*¹⁰⁶ SEU je definirao područje primjene zaštite osobnih podataka u kontekstu pristupa dokumentima institucija EU-a i odnos između uredbi (EZ) br. 1049/2001 (Uredba o pristupu dokumentima) i (EZ) br. 45/2001 (Uredba o zaštiti podataka u institucijama EU-a). Društvo Bavarian Lager, osnovano 1992., uvozi njemačko pivo u bocama u Ujedinjenu Kraljevinu, prvenstveno za pivnice i barove. Međutim, navedeno je društvo naišlo na prepreke jer je britansko zakonodavstvo

106 SEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd* [VW], 29. lipnja 2010.

de facto u povoljniji položaj stavljalo nacionalne proizvođače. Kao odgovor na žalbu društva Bavarian Lager, Europska komisija odlučila je pokrenuti postupak protiv Ujedinjene Kraljevine jer nije ispunila svoju obvezu, nakon čega su izmijenjene osporavane odredbe, koje su usklađene s pravom Unije. Bavarian Lager zatim je od Komisije, među ostalim dokumentima, zatražio i presliku zapisnika sa sastanka u kojemu su sudjelovali predstavnici Komisije, britanskih nadležnih tijela i udruženja *Confédération des Brasseurs du Marché Commun* (CBMC). Komisija je pristala otkriti određene dokumente povezane sa sastankom, no izostavila je pet imena koja su se pojavljivala u zapisniku jer su se dvije osobe izričito protivile otkrivanju identiteta, a Komisija nije uspjela kontaktirati preostala tri sudionika. Odlukom od 18. ožujka 2004. Komisija je odbila novi zahtjev društva Bavarian Lager za cjelovitim zapisnikom sa sastanka pozivajući se prvenstveno na zaštitu privatnog života pojedinaca zajamčenu Uredbom o zaštiti podataka u institucijama EU-a.

Budući da nije bilo zadovoljno iznesenim stavom, društvo Bavarian Lager podnijelo je tužbu Prvostupanjskom sudu. Taj je sud poništio odluku Komisije presudom od 8. studenoga 2007. (predmet T-194/04, *The Bavarian Lager Co. Ltd. protiv Komisije Europskih zajednica*) smatrajući da samo navođenje imena dotičnih osoba koje su predstavljale određena tijela na popisu sudionika sastanka nije narušavanje privatnog života niti dovodi privatne živote tih osoba u bilo kakvu opasnost.

Na žalbu Komisije SEU je poništio presudu Prvostupanjskog suda. SEU je smatrao da se Uredbom o pristupu dokumentima utvrđuje „poseban i pojačan sustav zaštite osobe čiji bi se osobni podaci mogli, ovisno o slučaju, otkriti javnosti”. Prema SEU-u, kada se zahtjevom koji se zasniva na Uredbi o pristupu dokumentima traži pristup dokumentima koji uključuju osobne podatke, u cijelosti se primjenjuju odredbe Uredbe o zaštiti podataka u institucijama EU-a. SEU je zatim zaključio da je Komisija s pravom odbila zahtjev za pristup cjelovitom sadržaju zapisnika sa sastanka iz listopada 1996. U nedostatku privole petero sudionika sastanka, Komisija je u dovoljnoj mjeri ispunila svoju dužnost otvorenosti dostavljajući verziju dokumenta u kojoj su izostavljena njihova imena.

Nadalje, prema SEU-u, „kako Bavarian Lager nije izričito i legitimno opravdao svoj zahtjev niti je pružio ikakav uvjerljiv argument kojim bi dokazao nužnost dostave tih osobnih podataka, Komisija nije mogla odvagati razne interese

dotičnih stranki, niti je mogla provjeriti je li bilo razloga za pretpostavku da se mogu ugroziti legitimni interesi ispitanika”, kako se zahtijeva Uredbom o zaštiti podataka u institucijama EU-a.

Primjer: U predmetu *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA)*¹⁰⁷ SEU je ispitao je li odluka Europske agencije za sigurnost hrane (EFSA) o uskraćivanju punog pristupa dokumentima tužiteljima bila nužna za zaštitu prava na privatnost i zaštitu podataka osoba na koje se u dokumentima upućivalo. Dokumenti su se odnosili na nacrt izvješća o smjernicama koji je pripremila radna skupina EFSA-e u suradnji s vanjskim stručnjacima u vezi sa stavljanjem fitosanitarnih proizvoda na tržište. EFSA je prvotno dodijelila djelomičan pristup tužiteljima i uskratila pristup određenim radnim verzijama nacrtu dokumenta sa smjernicama. Nakon toga je dodijelila pristup nacrtu koji je uključivao pojedinačne komentare vanjskih stručnjaka. Međutim, izostavila je imena stručnjaka pozivajući se na članak 4. stavak 1. točku (b) Uredbe (EZ) br. 45/2001 o obradi osobnih podataka u institucijama i tijelima EU-a te na potrebu za zaštitom privatnosti vanjskih stručnjaka. U prvostupanjskoj presudi Opći sud EU-a potvrdio je EFSA-inu odluku.

Nakon žalbe tužitelja SEU je poništio prvostupanjsku presudu. Zaključio je da je prijenos osobnih podataka u tom slučaju bio nužan za utvrđivanje nepristranosti svakog od vanjskih stručnjaka u njihovu obavljanju znanstvenih dužnosti te za osiguravanje transparentnosti postupka donošenja odluka u EFSA-i. Prema SEU-u, EFSA nije navela kako bi otkrivanje imena vanjskih stručnjaka koji su sastavili pojedine komentare o nacrtu dokumenta sa smjernicama utjecalo na legitimne interese tih stručnjaka. Opći argument da otkrivanje imena može narušiti privatnost nije dovoljan ako nije potkrijepljen dokazima specifičnima za svaki pojedini slučaj.

Prema ovim presudama, za miješanje u pravo na zaštitu podataka u kontekstu pristupa dokumentima potreban je određen i opravdan razlog. Pravom na pristup dokumentima ne može se automatski poništiti pravo na zaštitu podataka¹⁰⁸.

107 SEU, C-615/13 P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA) i Europske komisije*, 16. srpnja 2015.

108 Međutim, vidjeti detaljne rasprave u EDPS (2011.), *Public access to documents containing personal data after the Bavarian Lager ruling* (Javni pristup dokumentima koji sadrže osobne podatke nakon presude u predmetu Bavarian Lager), Bruxelles, 24. ožujka 2011.

Taj je pristup sličan pristupu ESLJP-a u pogledu privatnosti i pristupa dokumentima, kao što to pokazuje sljedeća presuda. U presudi *Magyar Helsinki* ESLJP je naveo da se člankom 10. pojedincima ne dodjeljuje pravo na pristup informacijama koje posjeduju javna tijela niti se obvezuje vlasti na pružanje takvih informacija pojedincima. Međutim, takvo pravo ili obveza može se pojaviti prvenstveno kada je otkrivanje informacija propisano sudskim nalogom koji je dobio pravnu snagu, zatim kada je pristup informacijama ključan za ostvarivanje prava pojedinca na slobodu izražavanja, a posebice slobodu primanja i širenja informacija, te kada bi se njihovim uskraćivanjem mijesalo u to pravo¹⁰⁹. Predstavlja li i u kojoj mjeri uskraćivanje pristupa informacijama mijesanje u slobodu izražavanja pojedinca mora se procijeniti u svakom pojedinačnom slučaju i u kontekstu njegovih posebnih okolnosti, uključujući sljedeće: (i) svrhu zahtjeva za informacije; (ii) prirodu informacija koje se traže; (iii) ulogu tužitelja; te (iv) spremnost i dostupnost informacija.

Primjer: U predmetu *Magyar Helsinki Bizottság protiv Mađarske*¹¹⁰ tužitelj, nevladina organizacija za zaštitu ljudskih prava, zatražio je informacije od policije u vezi s radom *ex officio* obrane da bi dovršio istraživanje o funkcioniranju sustava javnih pravobranitelja u Mađarskoj. Policija je odbila pružiti te informacije tvrdeći da su one osobni podaci koji ne podliježu objavi. Primjenjujući navedene kriterije, ESLJP je smatrao da je došlo do mijesanja u pravo zaštićeno člankom 10. Točnije, tužitelj je htio iskoristiti pravo na širenje informacija o pitanju od javnog interesa, tražio je pristup informacijama u tu svrhu te su informacije bile nužne za tužiteljevo iskorištavanje prava na slobodu izražavanja. Informacije o imenovanju javnih pravobranitelja bile su od interesa javnosti. Nije bilo razloga za sumnju da je navedeno istraživanje uključivalo informacije koje je tužitelj namjeravao objaviti i koje je javnost imala pravo primiti. Sud je stoga zaključio da je pristup traženim informacijama bio nužan da bi tužitelj ispunio zadatak. Naposljetku, informacije su bile spremne i dostupne.

ESLJP je zaključio da je uskraćivanjem pristupa informacijama u tom slučaju narušena suština slobode primanja informacija. U svrhu donošenja takva zaključka, razmotrio je posebno svrhu zatraženih informacija i njihov doprinos važnoj javnoj raspravi, prirodu traženih informacija i njihov potencijalni javni interes te položaj koji je tužitelj u ovom predmetu imao u društvu.

¹⁰⁹ ESLJP, *Magyar Helsinki Bizottság protiv Mađarske* [VV], br. 18030/11, 8. studenoga 2016., t. 148.

¹¹⁰ *Ibid.*, t. 181., od 187. do 200.

Sud je u obrazloženju napomenuo da se istraživanje koje je proveo NVO odnosilo na rad pravosuđa i pravo na pošteno saslušanje, što je jedno od prava temeljne važnosti prema EKLJP-u. Budući da zatražene informacije nisu uključivale podatke izvan javne domene, prava privatnosti ispitanika (*ex officio* javni pravobranitelji) ne bi bila narušena da je policija tužitelju odobrila pristup informacijama. Informacije koje je tužitelj zatražio bile su statistički podaci povezani s brojem slučajeva u kojima je *ex officio* obrana imenovana da predstavlja optuženike u javnim kaznenim postupcima.

Budući da se istraživanjem nastojalo pridonijeti važnoj raspravi o pitanju od općeg interesa, ESLJP je smatrao da su se sva ograničenja predložene objave NVO-a trebala podvrgnuti podrobnoj provjeri. Predmetne informacije bile su od javnog interesa s obzirom na to da javni interes obuhvaća „pitanja koja mogu uzrokovati znatne kontroverzije, pitanja koja se odnose na važan društveni problem ili pitanja koja uključuju problem koji bi mogao biti od interesa za javnost”¹¹¹. Stoga bi svakako obuhvaćao raspravu o provedbi pravosuđa i poštenih suđenja, što je bilo predmet istraživanja tužitelja. Odvagivanjem različitih prava i primjenom načela proporcionalnosti, ESLJP je zaključio da je došlo do neopravdanog kršenja prava tužitelja prema članku 10. EKLJP-a.

1.3.2. Poslovna tajna

Prema nacionalnom zakonodavstvu, određene komunikacije mogu podlijeagati obvezi čuvanja poslovne tajne. Poslovna tajna može se protumačiti kao posebna etička dužnost koja podrazumijeva pravnu obvezu svojstvenu određenim strukama i funkcijama koje se temelje na pouzdanju i povjerenju. Osobe i institucije koje obnašaju te funkcije obvezne su čuvati povjerljive podatke koje zaprimе prilikom obavljanja svojih dužnosti. Poslovna tajna prvenstveno se povezuje s medicinskom strukom i povjerljivošću komunikacije između odvjetnika i klijenta, a mnoge jurisdikcije priznaju obvezu čuvanja poslovne tajne i u financijskom sektoru. Poslovna tajna nije temeljno pravo, no zaštićena je kao oblik prava na poštovanje privatnog života. Primjerice, SEU je presudio da u određenim slučajevima postoji „potreba za zabranom otkrivanja određenih informacija koje su proglašene povjerljivima u svrhu očuvanja temeljnog prava poduzetnika na poštovanje privatnosti, kako je utvrđeno u članku 8. EKLJP-a i članku 7. Povelje”¹¹². ESLJP je također odlučivao o tome predstavljaju li

¹¹¹ *Ibid.*, t. 156.

¹¹² SEU, T-462/12 R, *Pilkington Group Ltd protiv Europske komisije*, Rješenje predsjednika Općeg suda, 11. ožujka 2013., t. 44.

ograničenja poslovne tajne kršenje članka 8. EKLJP-a, kako je opisano u sljedećim istaknutim primjerima.

Primjer: U predmetu *Pruteanu protiv Rumunjske*¹¹³ tužitelj je djelovao kao odvjetnik trgovačkog društva kojem je bilo zabranjeno izvršavanje bankovnih transakcija nakon optužbi za prijevare. Tijekom razmatranja predmeta rumunjski su sudovi odobrili tužiteljstvu da presretne i snima telefonske razgovore partnera društva tijekom određenog razdoblja. Snimke i presretnuti razgovori uključivali su komunikaciju s njegovim odvjetnikom.

Pruteanu je tvrdio da to predstavlja miješanje u njegovo pravo na poštovanje privatnog života i dopisivanje. ESLJP je u presudi istaknuo status i važnost odnosa odvjetnika s klijentom. Presretanjem razgovora odvjetnika s klijentom nedvojbeno je prekršena poslovna tajna, koja čini temelj odnosa između tih dviju osoba. U takvu slučaju odvjetnik također može uložiti pritužbu na miješanje u njegovo pravo na poštovanje privatnog života i dopisivanja. SEU je smatrao da je prekršen članak 8. EKLJP-a.

Primjer: U predmetu *Brito Ferrinho Bexiga Villa-Nova protiv Portugala*¹¹⁴ tužiteljica, inače odvjetnica, odbila je otkriti svoje osobne bankovne izvode poreznim tijelima na osnovi poslovne i bankovne tajne. Ured tužitelja pokrenuo je istragu zbog porezne prijevare i zatražio je odobrenje za obustavu poslovne tajne. Nacionalni sudovi izdali su nalog za obustavu pravila povjerljivosti i bankovne tajne, zaključivši da bi javni interes trebao prevagnuti nad osobnim interesima tužiteljice.

Kada je predmet došao do ESLJP-a, on je smatrao da je pristup bankovnim izvodima tužiteljice predstavljao miješanje u njezino pravo na poštovanje poslovne tajne, koje je obuhvaćeno konceptom privatnog života. Miješanje je imalo pravnu osnovu jer se temeljilo na zakoniku o kaznenom postupku i njime se nastojao ostvariti legitiman cilj. Međutim, preispitujući nužnost i proporcionalnost miješanja, ESLJP je istaknuo činjenicu da je postupak za ukidanje povjerljivosti proveden bez sudjelovanja ili znanja tužiteljice. Tužiteljica stoga nije mogla iznijeti svoje argumente. Usto, iako je nacionalnim zakonodavstvom propisano da je u takvu postupku potrebno savjetovanje s odvjetničkom komorom, ono nije provedeno. Naposljetku, tužiteljica nije

¹¹³ ESLJP, *Pruteanu protiv Rumunjske*, br. 30181/05, 3. veljače 2015.

¹¹⁴ ESLJP, *Brito Ferrinho Bexiga Villa-Nova protiv Portugala*, br. 69436/10, 1. prosinca 2015.

imala mogućnost učinkovito osporiti ukidanje povjerljivosti niti je imala na raspolaganju bilo kakav pravni lijek kojim bi osporila tu mjeru. Zbog izostanka postupovnih jamstava i učinkovitog sudskog nadzora nad mjerom kojom se obustavlja dužnost čuvanja povjerljivosti, ESLJP je zaključio da je došlo do kršenja članka 8. EKLJP-a.

Odnos između poslovne tajne i zaštite podataka često je dvoznačan. S jedne strane, propisi i mjere za zaštitu podataka utvrđeni zakonodavstvom pomažu u očuvanju poslovne tajne. Primjerice, propisima kojima se voditelji obrade i izvršitelji obrade obvezuju na uvođenje snažnih mjera za sigurnost podataka nastoji se, među ostalim, spriječiti gubitak povjerljivosti osobnih podataka zaštićenih poslovnom tajnom. Nadalje, Općom uredbom EU-a o zaštiti podataka omogućuje se obrada zdravstvenih podataka, koji čine posebnu kategoriju osobnih podataka, za koje je potrebna snažnija zaštita, no takva obrada istovremeno podliježe uspostavljanju primjerenih i posebnih mjera zaštite prava ispitanika, a posebno poslovne tajne¹¹⁵.

S druge strane, obvezama poslovne tajne nametnutima voditeljima obrade i izvršiteljima obrade u pogledu određenih osobnih podataka mogu se ograničiti prava ispitanika, a posebno pravo na primanje informacija. Iako Opća uredba o zaštiti podataka sadržava opsežan popis informacija koje se u načelu moraju pružiti ispitaniku ako osobni podaci nisu dobiveni od njega, taj zahtjev objave ne primjenjuje se kada osobni podaci moraju ostati povjerljivi zbog obveze poslovne tajne propisane nacionalnim zakonodavstvom ili zakonodavstvom EU-a¹¹⁶.

Općom uredbom o zaštiti podataka (OUZP) omogućuje se da države članice donesu posebne zakonske propise za zaštitu obveze poslovne tajne ili druge jednakovrijedne obveze tajnosti te da usklade pravo na zaštitu osobnih podataka s obvezom poslovne tajne¹¹⁷.

OUZP-om se propisuje da države članice mogu donijeti posebne propise o ovlastima nadzornih tijela u vezi s voditeljima obrade ili izvršiteljima obrade koji imaju obvezu čuvanja poslovne tajne. Ti posebni propisi povezani su s ovlasti ostvarivanja pristupa poslovnim prostorima voditelja obrade ili izvršitelja obrade, njihovoj opremi za obradu podataka i osobnim podacima koje posjeduju ako su takvi osobni podaci primljeni u okviru aktivnosti obuhvaćene obvezom tajnosti. Stoga nadzorna

¹¹⁵ Opća uredba o zaštiti podataka, članak 9. stavak 2. točka (h) i članak 9. stavak 3.

¹¹⁶ *Ibid.*, članak 14. stavak 5. točka (d).

¹¹⁷ *Ibid.*, uvodna izjava 164. i članak 90.

tijela nadležna za zaštitu podataka moraju poštovati obveze poslovne tajne koje se odnose na voditelje obrade i izvršitelje obrade. Nadalje, i članovi nadzornih tijela imaju dužnost čuvanja poslovne tajne tijekom i nakon svojeg mandata. U izvršavanju svojih zadataka članovi i osoblje nadzornih tijela mogu saznati određene povjerljive informacije. Člankom 54. stavkom 2. Uredbe jasno se propisuje da imaju dužnost čuvanja poslovne tajne u pogledu takvih povjerljivih informacija.

OUZP-om se od država članica zahtijeva da obavijeste Komisiju o pravilima koja donesu radi usklađivanja zaštite podataka i načela utvrđenih Uredbom s obvezom čuvanja poslovne tajne.

1.3.3. Sloboda vjeroispovijedi i uvjerenja

Sloboda vjeroispovijedi i uvjerenja zaštićena je člankom 9. EKLJP-a (sloboda mišljenja, savjesti i vjeroispovijedi) i člankom 10. Povelje EU-a o temeljnim pravima. Osobni podaci koji otkrivaju vjerska i filozofska uvjerenja smatraju se „osjetljivim podacima” prema pravu EU-a i Vijeća Europe te njihova obrada i upotreba podliježu pojačanoj zaštiti.

Primjer: Tužitelj u predmetu *Sinan Işık protiv Turske*¹¹⁸ bio je član vjerske zajednice alevita, čija su vjerovanja pod utjecajem sufizma i drugih predislamskih vjerovanja te koju neki akademski stručnjaci smatraju zasebnom religijom, a drugi dijelom islamske vjeroispovijedi. Tužitelj se žalio da je njegova identifikacijska iskaznica suprotno njegovim željama sadržavala polje u kojemu je njegova vjeroispovijed naznačena kao „islam” umjesto „alevizam”. Nacionalni su sudovi odbili njegov zahtjev za promjenu unosa na iskaznici u „alevizam” uz obrazloženje da ta riječ označava podskupinu islama, a ne zasebnu religiju. Zatim je podnio tužbu pred ESLJP-om u kojoj je naveo da je bio prisiljen javno obznaniti svoju vjeroispovijed bez privole jer je navođenje vjeroispovijedi na identifikacijskoj iskaznici bilo obvezno te da je time prekršeno njegovo pravo na slobodu vjeroispovijedi i savjesti, posebice kad se uzme u obzir da oznaka „islam” na iskaznici nije bila točna.

ESLJP je ponovio da sloboda vjeroispovijedi podrazumijeva slobodu izražavanja vjeroispovijedi u zajednici s drugim osobama, u javnosti te u krugu ljudi koji pripadaju istoj vjeroispovijedi, kao i u privatnosti i kada je osoba sama. Prema tadašnjem nacionalnom zakonodavstvu pojedinci su bili obvezani

¹¹⁸ ESLJP, *Sinan Işık protiv Turske*, br. 21924/05, 2. veljače 2010.

posjedovati identifikacijsku iskaznicu, dokument na kojemu je naznačena njihova vjeroispovijed, koju je trebalo predložiti na zahtjev bilo kojeg javnog tijela ili privatnog poduzeća. U sklopu te obveze nije uzeto u obzir da se pravom izražavanja vjeroispovijedi podrazumijeva i suprotno pravo, odnosno pravo na oslobođanje od obveze objave vjeroispovijedi. Iako je vlada tvrdila da je nacionalno zakonodavstvo izmijenjeno kako bi pojedinci mogli zatražiti da polje o vjeroispovijedi na identifikacijskoj kartici ostane prazno, prema mišljenju ESLJP-a, sama činjenica da je potrebno podnijeti zahtjev da se stavka vjeroispovijedi izbriše može predstavljati otkrivanje informacija o stavu prema religiji. Usto, kada identifikacijske iskaznice imaju polje o vjeroispovijedi, njegovo ostavljanje praznim ima specifične konotacije jer bi se vlasnici identifikacijskih iskaznica bez informacija o vjeroispovijedi isticali među onima na čijoj je iskaznici ta stavka navedena. ESLJP je zaključio da se nacionalnim zakonodavstvom krši članak 9. EKLJP-a.

Međutim, za rad crkvi i vjerskih udruga ili zajednica može biti potrebna obrada osobnih podataka članova kako bi se omogućila komunikacija i organizacija aktivnosti u zajednici vjernika. Stoga crkve i vjerske udruge često uvode pravila obrade osobnih podataka. Prema članku 91. Opće uredbe o zaštiti podataka, kada su takva pravila sveobuhvatna, mogu i dalje biti važeća pod uvjetom da se usklade s odredbama Uredbe. Crkve i vjerske udruge koje imaju takva pravila moraju se podvrgnuti nadzoru neovisnog nadzornog tijela, koje može biti posebno nadležno za njih, pod uvjetom da ispunjavaju uvjete Opće uredbe o zaštiti podataka za takva tijela¹¹⁹.

Vjerske organizacije mogu obrađivati osobne podatke iz nekoliko razloga, primjerice radi održavanja kontakta s vjernicima ili prenošenja informacija o vjerskim ili dobrotvornim događanjima i proslavama koje organiziraju. U određenim državama crkve moraju voditi registre članova zbog poreznih razloga, s obzirom na to da broj članova vjerskih ustanova može utjecati na iznos poreza koje pojedinci trebaju plaćati. U svakom slučaju, prema europskom pravu, podaci koji otkrivaju religijska uvjerenja pojedinaca smatraju se osjetljivim podacima i crkve moraju snositi odgovornost za rukovanje takvim podacima i njihovu obradu, posebice s obzirom na to da se informacije koje obrađuju vjerske organizacije često odnose na djecu, starije osobe ili druge osjetljive skupine u društvu.

¹¹⁹ Opća uredba o zaštiti podataka, članak 91. stavak 2.

1.3.4. Sloboda umjetnosti i znanosti

Sloboda umjetnosti i znanosti, koja je izričito zaštićena člankom 13. Povelje EU-a o temeljnim pravima, još je jedno pravo koje valja odvagati u odnosu na prava na poštovanje privatnog života i zaštitu podataka. To je pravo u prvom redu izvedeno iz prava na slobodu mišljenja i izražavanja, a njegovo ostvarivanje podliježe članku 1. Povelje (ljudsko dostojanstvo). ESLJP smatra da je sloboda umjetnosti zaštićena člankom 10. Europske konvencije o ljudskim pravima¹²⁰. Pravo zajamčeno člankom 13. Povelje može podlijezati i ograničenjima iz članka 52. stavka 1. Povelje, koji se može tumačiti i iz perspektive članka 10. stavka 2. EKLJP-a¹²¹.

Primjer: U predmetu *Vereinigung bildender Künstler protiv Austrije*¹²² austrijski sudovi zabranili su udruzi tužiteljici daljnje izlaganje slike s fotografijama glava različitih javnih ličnosti u seksualnim pozama. Austrijski član parlamenta čija je fotografija također iskorištena na slici pokrenuo je postupak protiv udruge tužiteljice, tražeći zabranu izlaganja slike. Nacionalni je sud dosudio zabranu. ESLJP je ponovio da se članak 10. EKLJP-a primjenjuje na širenje ideja koje vrijeđaju, izazivaju šok ili uznemiruju državu ili bilo koji dio populacije. Oni koji stvaraju, izvode, šire ili izlažu umjetnička djela pridonose razmjeni ideja i mišljenja i država je dužna ne uskratiti im nepotrebno slobodu izražavanja. Budući da je predmetna slika bila kolaž u kojem su iskorištene samo glave osoba, a njihova su tijela oslikana na nerealističan i pretjeran način, čija svrha očito nije bila predstavljanje, pa čak ni nagovještaj stvarnosti, ESLJP je nadalje izjavio da se „slika teško može tumačiti kao da se tiče privatnog života [dotičnog], već se ona prije tiče njegova javnog položaja političara” te da je „u tom svojstvu [dotični] trebao pokazati više tolerancije na kritiku”. Odvagujući različite interese, ESLJP je zaključio da je neograničena zabrana daljnjeg izlaganja slike neproporcionalna. ESLJP je stoga zaključio da je došlo do kršenja članka 10. Konvencije.

Europsko zakonodavstvo o zaštiti podataka uzima u obzir i posebnu vrijednost koju znanost ima za društvo. Općom uredbom o zaštiti podataka i moderniziranom Konvencijom br. 108 dopušta se zadržavanje podataka tijekom duljih razdoblja ako će se osobni podaci upotrebljavati isključivo u svrhu znanstvenih ili povijesnih istraživanja. Nadalje, neovisno o izvornoj svrsi određene aktivnosti obrade, daljnja uporaba

¹²⁰ ESLJP, *Müller i drugi protiv Švicarske*, br. 10737/84, 24. svibnja 1988.

¹²¹ Objašnjenja koja se odnose na Povelju Europske unije o temeljnim pravima, SL 2007 C 303.

¹²² ESLJP, *Vereinigung bildender Künstler protiv Austrije*, br. 68354/01, 25. siječnja 2007., t. 26. i 34.

osobnih podataka u znanstvenim istraživanjima ne smatra se neprikladnom svrhom¹²³. Istovremeno se moraju provesti odgovarajuće zaštitne mjere za takvu obradu kako bi se zaštitila prava i slobode ispitanika. U pravu EU-a ili država članica mogu se propisati izuzeća za prava ispitanika, primjerice prava na pristup, ispravak, ograničenje obrade i prigovor u vezi s obradom njihovih osobnih podataka u svrhu znanstvenih istraživanja te u povijesne ili statističke svrhe (vidjeti također [dio 6.1.](#) i [dio 9.4.](#)).

1.3.5. Zaštita intelektualnog vlasništva

Pravo na zaštitu vlasništva sadržano je u članku 1. Prvog protokola uz Europsku konvenciju o ljudskim pravima te u članku 17. stavku 1. Povelje EU-a o temeljnim pravima. Jedan od aspekata prava na vlasništvo koji je posebno značajan za zaštitu podataka zaštita je intelektualnog vlasništva, koja se izričito spominje u članku 17. stavku 2. Povelje. U pravnom poretku EU-a postoji nekoliko direktiva donesenih u svrhu učinkovite zaštite intelektualnog vlasništva i to osobito autorskog prava. Intelektualno vlasništvo ne obuhvaća samo literarno i umjetničko vlasništvo već i patente, žigove i srodna prava.

Iz sudske prakse SEU-a jasno proizlazi da se zaštita temeljnog prava na vlasništvo mora uravnotežiti sa zaštitom drugih temeljnih prava, osobito prava na zaštitu podataka¹²⁴. Bilo je slučajeva kada su institucije za zaštitu autorskih prava od davatelja usluga internetskog pristupa tražile da otkriju identitet korisnika internetskih platformi za zajedničko korištenje datotekama. Takve platforme naime korisnicima interneta često omogućuju besplatno preuzimanje glazbenih zapisa unatoč tome što su zaštićeni autorskim pravom.

Primjer: Predmet *Promusicae protiv Telefónica de España*¹²⁵ odnosio se na protivljenje društva Telefónica, španjolskog pružatelja usluga internetskog pristupa, da osobne podatke nekolicine osoba kojima je pružao usluge internetskog pristupa otkrije neprofitnoj organizaciji glazbenih producenata i izdavača glazbenih i audiovizualnih snimki pod nazivom Promusicae. Organizacija Promusicae zatražila je otkrivanje informacija kako bi mogla pokrenuti

123 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (b) i modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b).

124 SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. siječnja 2008., t. od 62. do 68.

125 *Ibid.*, t. 54. i 60.

građanski postupak protiv tih osoba, za koje je tvrdila da su upotrebljavale program razmjene datoteka s pristupom fonogramima na koje su pravo upotrebe polagali članovi organizacije Promusicae.

Španjolski je sud predmet proslijedio SEU-u zatraživši odgovor na pitanje moraju li se, prema pravu Zajednice, takvi osobni podaci priopćiti u kontekstu građanskih parnica kako bi se osigurala učinkovita zaštita autorskog prava. Pozvao se na direktive 2000/31, 2001/29 i 2004/48, tumačene i u kontekstu članaka 17. i 47. Povelje. Sud je zaključio da te tri direktive, kao i Direktiva o privatnosti i elektroničkim komunikacijama (Direktiva 2002/58/EZ), ne sprečavaju države članice da propišu obvezu otkrivanja osobnih podataka u kontekstu građanskih parnica radi učinkovite zaštite autorskog prava.

SEU je istaknuo da je slučaj potaknuo pitanje potrebe za usklađivanjem zahtjeva za zaštitu različitih temeljnih prava, odnosno prava na poštovanje privatnog života i prava na zaštitu vlasništva i djelotvoran pravni lijek.

Zaključio je da se „države članice kod prenošenja navedenih direktiva moraju skrbiti o tome da ih tumače na način koji omogućava osiguranje pravedne ravnoteže između različitih temeljnih prava koja su zaštićena pravnim poretkom Zajednice. Nadalje, prilikom provedbe mjera za prenošenje navedenih direktiva, na tijelima i sudovima država članica jest dužnost ne samo da svoje nacionalno pravo tumače u skladu s tim direktivama, nego i da ih ne tumače na način koji bi bio protivan navedenim temeljnim pravima ili drugim općim načelima prava Zajednice, kao što je načelo proporcionalnosti”¹²⁶.

Primjer: Predmet *Bonnier Audio AB i drugi protiv Perfect Communication Sweden AB*¹²⁷ odnosio se na ravnotežu između prava intelektualnog vlasništva i zaštite osobnih podataka. Tužitelji – pet izdavačkih kuća koje su bile nositelji autorskih prava na 27 audioknjiga – pokrenuli su postupak pred švedskim sudom navodeći da su ta autorska prava prekršena putem FTP poslužitelja (protokola za prijenos podataka koji omogućuje dijeljenje datoteka i prijenos podataka putem interneta). Tužitelji su od pružatelja internetskih usluga (ISP) zatražili da otkrije ime i adresu osobe koja se koristila IP adresom s koje su

¹²⁶ Ibid., t. 65. i 68; vidjeti i SEU, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) protiv Netlog NV*, 16. veljače 2012.

¹²⁷ SEU, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB protiv Perfect Communication Sweden AB*, 19. travnja 2012.

poslane datoteke. Pružatelj usluga, društvo ePhone, osporilo je taj zahtjev navodeći da se njime krši Direktiva 2006/24/EZ (Direktiva o zadržavanju podataka, proglašena nevažećom 2014.).

Švedski sud prosljedio je predmet SEU-u uz pitanje sprečava li Direktiva 2006/24/EZ primjenu nacionalne odredbe koja se temelji na članku 8. Direktive 2004/48/EZ (Direktiva o provedbi prava intelektualnog vlasništva), kojim se omogućuje izdavanje sudskog naloga kojim se zahtijeva da ISP-i prenesu informacije nositeljima autorskih prava o pretplatnicima čije su IP adrese navodno upotrijebljene za kršenje prava. To se pitanje temeljilo na pretpostavci da je tužitelj iznio jasne dokaze o kršenju određenog autorskog prava i da je mjera proporcionalna.

SEU je istaknuo da se Direktiva 2006/24/EZ odnosi isključivo na rukovanje podacima i zadržavanje podataka koje proizvedu pružatelji elektroničkih komunikacijskih usluga u svrhu istrage, otkrivanja i progona teških kaznenih djela te na njihovo prenošenje nadležnim nacionalnim tijelima. Stoga se nacionalna odredba kojom se Direktiva o provedbi prava intelektualnog vlasništva prenosi u nacionalno zakonodavstvo nalazi izvan područja primjene Direktive 2006/24/EZ, i stoga nije onemogućena tom direktivom¹²⁸.

Kad je riječ o prenošenju imena i adrese koje su tražili tužitelji, SEU je smatrao da takav postupak predstavlja obradu osobnih podataka i pripada području primjene Direktive 2002/58/EZ (Direktiva o privatnosti i elektroničkim komunikacijama). Također je napomenuo da je prenošenje takvih podataka potrebno u građanskim parnicama kako bi se nositelju autorskog prava osigurala učinkovita zaštita autorskih prava, te stoga, zbog svoje svrhe, također pripada području primjene Direktive 2004/48/EZ¹²⁹.

SEU je zaključio da se direktive 2002/58/EZ i 2004/48/EZ moraju tumačiti tako da ne sprečavaju nacionalno zakonodavstvo poput onoga koje se navodi u glavnom postupku ako se takvim zakonodavstvom nacionalnom sudu koji odlučuje o zahtjevu za izdavanje naloga za otkrivanje osobnih podataka omogućuje da odvagne sukobljene interese na temelju činjenica svakog pojedinog slučaja i uzimajući u obzir zahtjeve načela proporcionalnosti.

¹²⁸ *Ibid.*, t. 40. i 41.

¹²⁹ *Ibid.*, t. od 52. do 54. Vidjeti i SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. siječnja 2008., t. 58.

1.3.6. Zaštita podataka i gospodarski interesi

U dobu digitalnih tehnologija ili velikih podataka podaci se nazivaju „novom naftom“ jer potiču gospodarske inovacije i kreativnost¹³⁰. Mnoga su društva izgradila snažne poslovne modele na obradi podataka, koja obično uključuje osobne podatke. Određena društva smatraju da pojedina pravila povezana sa zaštitom osobnih podataka u praksi mogu uzrokovati preopterećenje obvezama koje mogu utjecati na njihove gospodarske interese. Stoga se postavlja pitanje mogu li gospodarski interesi voditelja obrade i izvršitelja obrade ili šire javnosti opravdati ograničavanje prava na zaštitu podataka.

Primjer: U predmetu *Google Spain*¹³¹ SEU je smatrao da u određenim uvjetima pojedinci imaju pravo zatražiti da internetske tražilice uklone rezultate pretraživanja iz svojih indeksa za traženje. U obrazloženju je istaknuo činjenicu da se uporabom internetskih tražilica i navedenih rezultata pretraživanja može utvrditi detaljan profil pojedinca. Te se informacije mogu odnositi na brojne aspekte privatnog života osobe i ne mogu se jednostavno pronaći ili povezati bez internetske tražilice. Takvi postupci stoga čine potencijalno ozbiljno miješanje u temeljna prava na privatnost i zaštitu osobnih podataka ispitanika.

SEU je zatim ispitao može li se to miješanje opravdati. U pogledu gospodarskog interesa društva vlasnika internetske tražilice za obradu podataka SEU je naveo: „nužno je ustvrditi da [miješanje] ne može biti opravdano samo ekonomskim interesom operatera takvog pretraživača u toj obradi“ te da „načelno“ temeljna prava iz članaka 7. i 8. Povelje imaju prevagu nad takvim gospodarskim interesom i nad interesom javnosti u vezi s pronalaženjem navedene informacije prilikom pretrage imena ispitanika¹³².

Jedno od ključnih pitanja europskog zakonodavstva o zaštiti podataka jest pružanje veće kontrole pojedincima nad vlastitim osobnim podacima. U digitalnom je dobu posebno prisutna neravnoteža između ovlasti poslovnih subjekata koji obrađuju podatke i imaju pristup znatnim količinama osobnih podataka i ovlasti pojedinaca

130 Primjerice, vidjeti *Financial Times* (2016.), „Data is the new oil... who's going to own it?“, 16. studenoga 2016.

131 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014.

132 *Ibid.*, t. 81. i 97.

kojima ti osobni podaci pripadaju da kontroliraju vlastite podatke. SEU svakom predmetu pristupa pojedinačno kada odvaguje zaštitu podataka i gospodarske interese, poput interesa trećih strana u vezi s dioničkim društvima i društvima s ograničenom odgovornošću, kao što je vidljivo u presudi u predmetu *Manni*.

Primjer: Predmet *Manni*¹³³ odnosio se na uvrštavanje osobnih podataka pojedinca u javni trgovački registar. G. Manni zatražio je od Gospodarske komore Grada Leccea u Italiji da izbriše njegove osobne podatke iz tog registra nakon što je otkrio da bi potencijalni klijenti pretraživali registar i saznali da je bio upravitelj društva koje je proglasilo stečaj više od desetljeća ranije. Te su informacije utjecale na mišljenje njegovih potencijalnih klijenata i mogle su se negativno odraziti na njegove komercijalne interese.

Od SEU-a se tražilo da utvrdi priznaje li se pravom EU-a pravo na brisanje u tom slučaju. U donošenju zaključka SEU je odvagao propise EU-a o zaštiti podataka i komercijalne interese g. Mannija za uklanjanje informacija o stečaju njegova prijašnjeg društva s javnim interesom za pristup tim informacijama. Uzeo je u obzir činjenicu da je objava u javnom registru trgovačkih društava propisana zakonom, a posebice direktivom EU-a kojoj je svrha učiniti podatke o društvima dostupnijima trećim stranama. Objava je važna radi zaštite interesa trećih strana koje žele poslovati s određenim društvom, s obzirom na to da je jedina zaštitna mjera koju dionička društva i društva s ograničenom odgovornošću pružaju trećim stranama njihova imovina. Stoga „bi osnovni dokumenti trgovačkog društva trebali biti objavljeni kako bi treće strane mogle provjeriti njihove sadržaje i druge informacije koje se odnose na trgovačko društvo, posebno pojedinosti o osobama koje su ovlaštene obvezati trgovačko društvo”¹³⁴.

S obzirom na važnost legitimnog cilja koji se nastojao postići registrom, SEU je smatrao da g. Manni nije imao pravo na brisanje svojih osobnih podataka jer je potreba za zaštitom interesa trećih strana u odnosu na dionička društva i društva s ograničenom odgovornošću, kao i za osiguravanjem pravne sigurnosti, poštenosti poslovanja i pravilnog funkcioniranja unutarnjeg tržišta, imala prednost nad njegovim pravima na temelju zakonodavstva o zaštiti podataka. To je posebno točno kada se u obzir uzme činjenica da su pojedinci

133 SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. ožujka 2017.

134 *Ibid.*, t. 49.

koji odluče sudjelovati u trgovini putem dioničkog društva ili društva s ograničenom odgovornošću svjesni da moraju otkriti podatke o svojem identitetu i funkcijama.

Iako je zaključio da nije bilo osnove za brisanje podataka u ovom slučaju, SEU je priznao da postoji pravo na prigovor na obradu, tvrdeći da „se ne može isključiti mogućnost postojanja određenih situacija u kojima jaki i zakoniti razlozi u vezi s konkretnim slučajem predmetne osobe iznimno opravdavaju ograničavanje pristupa osobnim podacima koji se na nju odnose, upisanih u registar, po isteku dovoljno dugog roka [...] trećim osobama koje imaju konkretan interes za uvid u njih”¹³⁵.

SEU je ustvrdio da je na nacionalnim sudovima da, uzimajući u obzir sve relevantne okolnosti pojedinca, u svakom predmetu procijene postojanje ili nepostojanje zakonitih i jakih razloga kojima bi se iznimno opravdalo ograničenje pristupa trećih strana osobnim podacima sadržanima u registrima trgovačkih društava. Međutim, obrazložio je da se u slučaju g. Mannija činjenica da je otkrivanje njegovih osobnih podataka u registru navodno utjecalo na njegove klijente sama po sebi ne može smatrati takvim, zakonitim i jakim razlogom. Potencijalni klijenti g. Mannija imaju zakonit interes za informacije o stečaju njegova prijašnjeg društva.

Miješanje u temeljna prava g. Mannija i drugih osoba uvrštenih u registar na poštovanje privatnog života i zaštitu osobnih podataka, zajamčena člancima 7. i 8. Povelje, poslužilo je cilju od općeg interesa te je bilo nužno i proporcionalno.

Stoga je u predmetu *Manni* SEU zaključio da prava na zaštitu podataka i privatnost nisu prevagnula nad interesom trećih strana za pristup informacijama u registru trgovačkih društava koje se odnose na dionička društva i društva s ograničenom odgovornošću.

¹³⁵ *Ibid.*, t. 60.

2

Terminologija povezana sa zaštitom podataka

EU	Obuhvaćena pitanja	Vijeće Europe
Osobni podaci		
Opća uredba o zaštiti podataka, članak 4. stavak 1.	Pravna definicija zaštite podataka	Modernizirana Konvencija br. 108, članak 2. točka (a)
Opća uredba o zaštiti podataka, članak 4. stavak 5. i članak 5. stavak 1. točka (e)		ESLJP, <i>Bernh Larsen Holding AS i drugi protiv Norveške</i> , br. 24117/08, 2013.
Opća uredba o zaštiti podataka, članak 9.		ESLJP, <i>Uzun protiv Njemačke</i> , br. 35623/05, 2010.
SEU, spojeni predmeti C-92/09 i C-93/09, <i>Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen</i> [VV], 2010.		ESLJP, <i>Amann protiv Švicarske</i> [VV], br. 27798/95, 2000.
SEU, C-275/06, <i>Productores de Música de España (Promusicae) protiv Telefónica de España SAU</i> [VV], 2008.		
SEU, C-70/10, <i>Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)</i> , 2011.		
SEU, C-582/14, <i>Patrick Breyer protiv Bundesrepublik Deutschland</i> , 2016.		
SEU, spojeni predmeti C-141/12 i C-372/12, <i>Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.</i> , 2014.		

EU	Obuhvaćena pitanja	Vijeće Europe
SEU, C-101/01, <i>Kazneni postupak protiv Bodil Lindqvist</i> , 2003.	Posebne kategorije osobnih podataka (osjetljivi podaci)	Modernizirana Konvencija br. 108, članak 6. stavak 1.
SEU, C-434/16, <i>Peter Nowak protiv Data Protection Commissioner</i> , 2017.	Anonimizirani i pseudo-nimizirani osobni podaci	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (e) Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 50.
Obrada podataka		
Opća uredba o zaštiti podataka, članak 4. stavak 2. SEU, C-212/13, <i>František Ryneš protiv Úřad pro ochranu osobních údajů</i> , 2014. SEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija</i> , 2017. SEU, C-101/01, <i>Kazneni postupak protiv Bodil Lindqvist</i> , 2003. SEU, C-131/12, <i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González</i> [VV], 2014.	Definicije	Modernizirana Konvencija br. 108, članak 2. točke (b) i (c)
Korisnici podataka		
Opća uredba o zaštiti podataka, članak 4. stavak 7. SEU, C-212/13, <i>František Ryneš protiv Úřad pro ochranu osobních údajů</i> , 2014. SEU, C-1318/12, <i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González</i> [VV], 2014.	Voditelj obrade	Modernizirana Konvencija br. 108, članak 2. točka (d) Profiling Recommendation (Preporuka o izradi profila), članak 1. točka (g)*
Opća uredba o zaštiti podataka, članak 4. stavak 8.	Izvršitelj obrade	Modernizirana Konvencija br. 108, članak 2. točka (f) Preporuka o izradi profila, članak 1. točka (h)
Opća uredba o zaštiti podataka, članak 4. stavak 9.	Primatelj	Modernizirana Konvencija br. 108, članak 2. točka (e)
Opća uredba o zaštiti podataka, članak 4. stavak 10.	Treća strana	

EU	Obuhvaćena pitanja	Vijeće Europe
Privola		
Opća uredba o zaštiti podataka, članak 4. stavak 11. i članak 7. SEU, C-543/09, <i>Deutsche Telekom AG protiv Bundesrepublik Deutschland</i> , 2011. SEU, C-536/15, <i>Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)</i> , 2017.	Definicije i zahtjevi za valjanu privolu	Modernizirana Konvencija br. 108, članak 5. stavak 2. Medical Data Recommendation (Preporuka o medicinskim podacima), članak 6. i razne daljnje preporuke ESLJP, <i>Elberte protiv Latvije</i> , br. 61243/08, 2015.

Napomena: * Vijeće Europe, Odbor ministara (2010.), Preporuka CM/Rec(2010)13 državama članicama o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila (Preporuka o izradi profila), 23. studenoga 2010.

2.1. Osobni podaci

Ključne točke

- Podaci su osobni ako se odnose na osobu utvrđenog identiteta ili osobu čiji se identitet može utvrditi, odnosno „ispitanika”.
- Kako bi se odredilo može li se identitet pojedinca utvrditi, voditelj obrade ili bilo koja druga osoba trebali bi uzeti u obzir sva sredstva – poput selekcije – za koja je vjerojatno da mogu biti upotrijebljena u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca.
- Autentifikacija je postupak dokazivanja da određena osoba ima određeni identitet i/ili je ovlaštena za poduzimanje određenih radnji.
- Postoje posebne kategorije podataka, takozvani osjetljivi podaci, navedeni u moderniziranoj Konvenciji br. 108 i u zakonodavstvu EU-a o zaštiti podataka, koji zahtijevaju pojačanu zaštitu, te stoga podliježu posebnom pravnom režimu.
- Podaci su anonimizirani ako se više ne odnose na osobu utvrđenog identiteta ili osobu čiji se identitet može utvrditi.
- Pseudonimizacija je mjera prema kojoj se osobni podaci ne mogu pripisati ispitaniku bez dodatnih informacija, koje se čuvaju odvojeno. „Ključ” koji omogućuje naknadnu identifikaciju ispitanika mora se čuvati odvojeno i na sigurnom. Podaci nad kojima je izvršen postupak pseudonimizacije ostaju osobni podaci. U pravu EU-a ne postoji koncept „pseudonimiziranih podataka”.
- Načela i pravila zaštite podataka ne primjenjuju se na anonimizirane podatke, no primjenjuju se na pseudonimizirane podatke.

2.1.1. Glavni aspekti koncepta osobnih podataka

Na temelju prava EU-a, kao i **na temelju prava Vijeća Europe**, „osobni podaci” definirani su kao informacije koje se odnose na identificiranu fizičku osobu ili fizičku osobu koju se može identificirati¹³⁶. To se odnosi na informacije o osobi čiji je identitet sasvim jasan ili ga je barem moguće utvrditi uz dodatne informacije. Kako bi se odredilo može li se identitet pojedinca utvrditi, voditelj obrade ili bilo koja druga osoba mora uzeti u obzir sva sredstva koja se po svemu sudeći mogu upotrijebiti u svrhu izravnog ili neizravnog utvrđivanja identiteta pojedinca, poput primjerice selekcije, koja omogućuje da se s jednom osobom postupa drugačije od drugih¹³⁷.

Ako se podaci o takvoj osobi obrađuju, ona se naziva „ispitanik”.

Ispitanik

Na temelju prava EU-a, fizičke osobe jedini su korisnici propisa za zaštitu podataka¹³⁸ i samo su živa bića zaštićena europskim zakonodavstvom o zaštiti podataka¹³⁹. U Općoj uredbi o zaštiti podataka (OUZP) osobni se podaci definiraju kao svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.

U pravu Vijeća Europe, posebno u moderniziranoj Konvenciji br. 108, također se upućuje na zaštitu pojedinaca u pogledu obrade njihovih osobnih podataka. I u njoj osobni podaci označavaju sve podatke koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Ta fizička osoba, ili pojedinac, kako se naziva u OUZP-u odnosno moderniziranoj Konvenciji br. 108, u zakonodavstvu o zaštiti podataka poznata je kao ispitanik.

Pravne osobe također imaju pravo na određenu zaštitu. Postoji sudska praksa ESLJP-a s presudama u tužbama pravnih osoba zbog navodnog kršenja njihova prava na zaštitu od uporabe njihovih podataka sukladno članku 8. EKLJP-a. Člankom 8. EKLJP-a obuhvaćaju se pravo na poštovanje privatnog i obiteljskog života te pravo na poštovanje doma i dopisivanja. Sud stoga može razmatrati predmete u okviru poto-njeg, a ne u okviru privatnog života.

¹³⁶ Opća uredba o zaštiti podataka, članak 4. stavak 1.; modernizirana Konvencija br. 108, članak 2. točka (a).

¹³⁷ Opća uredba o zaštiti podataka, uvodna izjava 26.

¹³⁸ *Ibid.*, članak 1.

¹³⁹ *Ibid.*, uvodna izjava 27. Vidjeti i Radna skupina iz članka 29. (2007.), *Opinion 4/2007 on the concept of personal data* (Mišljenje 4/2007 o konceptu osobnih podataka), WP 136, 20. lipnja 2007., str. 22.

Primjer: Predmet *Bernh Larsen Holding AS i drugi protiv Norveške*¹⁴⁰ odnosio se na žalbu triju norveških društava na odluku poreznog tijela koja im je nalagala da poreznim revizorima dostave preslike svih podataka s računalnog poslužitelja koji su zajednički upotrebljavala.

ESLJP je smatrao da je takva obveza nametnuta društvima tužiteljima predstavljala miješanje u njihova prava na poštovanje „doma“ i „dopisivanja“ iz članka 8. EKLJP-a. Međutim, ESLJP je zaključio da su porezna tijela raspolagala odgovarajućim i učinkovitim mehanizmima zaštite od zlouporabe: društva tužitelji obaviještena su dovoljno unaprijed, bila su prisutna i mogla su sudjelovati u postupku tijekom intervencije na licu mjesta, a materijal se trebao uništiti po završetku porezne revizije. U tim je okolnostima postignuta pravedna ravnoteža između prava društava tužitelja na poštovanje „doma“ i „dopisivanja“ te njihova interesa povezanog sa zaštitom privatnosti njihovih zaposlenika s jedne strane i javnog interesa učinkovite inspekcije radi porezne procjene s druge strane. ESLJP je zaključio da stoga nije došlo do kršenja članka 8.

Prema moderniziranoj Konvenciji br. 108, zaštita podataka u prvom se redu bavi zaštitom fizičkih osoba, no ugovorne stranke u okviru nacionalnog zakonodavstva mogu proširiti zaštitu podataka i na pravne osobe, primjerice poduzeća i udruge. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da se nacionalnim zakonodavstvom mogu zaštititi legitimni interesi pravnih osoba proširivanjem područja primjene Konvencije na takve osobe¹⁴¹. **Zakonodavstvo EU-a o zaštiti podataka** ne obuhvaća obradu osobnih podataka koji se tiču pravnih osoba, a osobito ne poduzetnika koji su uspostavljeni kao pravne osobe, uključujući ime i oblik pravne osobe i kontaktne podatke pravne osobe¹⁴². Međutim, Direktivom o privatnosti i elektroničkim komunikacijama štite se povjerljivost komunikacija i legitimni interesi pravnih osoba u pogledu povećanja kapaciteta automatske pohrane i obrade podataka povezanih s pretplatnicima i korisnicima¹⁴³. Slično tome, nacrtom Uredbe o e-privatnosti zaštita se proširuje na pravne osobe.

140 ESLJP, *Bernh Larsen Holding AS i drugi protiv Norveške*, br. 24117/08, 14. ožujka 2013. Vidjeti i ESLJP, *Liberty i drugi protiv Ujedinjene Kraljevine*, br. 58243/00, 1. srpnja 2008.

141 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 30.

142 Opća uredba o zaštiti podataka, uvodna izjava 14.

143 Direktiva o privatnosti i elektroničkim komunikacijama, uvodna izjava 7. i članak 1. stavak 2.

Primjer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*¹⁴⁴ SEU je, pozivajući se na objavu osobnih podataka o korisnicima poljoprivredne potpore, smatrao da se „pravne osobe mogu pozvati na zaštitu iz članka 7. i 8. Povelje samo ako tvrtka pravne osobe upućuje na jednu ili više fizičkih osoba. [...] [P]oštovanje prava na privatni život s obzirom na obradu osobnih podataka, koje je priznato člancima 7. i 8. Povelje, odnosi se na svaku informaciju koja se tiče fizičke osobe čiji je identitet utvrđen ili se može utvrditi [...]”¹⁴⁵.

Odvagivanjem interesa EU-a da osigura transparentnost u dodjeli potpora s jedne strane i temeljnih prava na privatnost i zaštitu podataka pojedinaca koji se koriste potporama s druge strane, SEU je zaključio da je miješanje u ta temeljna prava bilo neproporcionalno. Smatrao je da se cilj transparentnosti mogao učinkovito ostvariti mjerama koje su manje nametljive u pogledu prava dotičnih pojedinaca. Međutim, prilikom razmatranja proporcionalnosti objave informacija o pravnim osobama koje su primile potporu, SEU je došao do drugačijeg zaključka, presudivši da takvom objavom nisu prekoračena ograničenja načela proporcionalnosti. Utvrdio je da se „ozbiljnost povrede prava na zaštitu osobnih podataka iskazuje na različite načine za pravne osobe s jedne strane i fizičke osobe s druge”¹⁴⁶. Pravne osobe podliježu strožim obvezama u vezi s objavom informacija o njima. SEU je smatrao da bi se zahtijevanjem da nacionalna tijela ispituju može li se podacima svake pravne osobe koja je korisnica potpora identificirati bilo koja s njom povezana fizička osoba prije objave tih podataka tim tijelima nametnulo nerazumno administrativno opterećenje. Stoga je zakonodavstvom kojim se zahtijeva opća objava podataka o pravnim osobama uspostavljena pravedna ravnoteža između navedenih sukobljenih interesa.

Priroda podataka

Svaka informacija može biti osobni podatak pod uvjetom da se odnosi na identificiranu osobu ili osobu koju se može identificirati.

¹⁴⁴ SEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010., t. 53.

¹⁴⁵ *Ibid.*, t. 52. i 53.

¹⁴⁶ *Ibid.*, t. 87.

Primjer: Procjena radnih sposobnosti djelatnika koju nadređeni pohranjuje u osobni dosje djelatnika osobni je podatak o djelatniku. To je slučaj čak i ako podaci sadržavaju, djelomice ili u cijelosti, samo osobno mišljenje nadređenog, primjerice: „Djelatnik nije posvećen poslu“, a ne konkretne činjenice kao što je: „Djelatnik je u proteklih šest mjeseci s posla izostao pet tjedana.“

Osobni podaci obuhvaćaju informacije koje se tiču privatnog života osobe, što uključuje i profesionalne aktivnosti, kao i informacije o njezinu javnom životu.

U predmetu *Amann*¹⁴⁷ ESLJP je pojam „osobni podaci“ tumačio ne ograničavajući ga na pitanja privatne sfere pojedinca. To je značenje pojma „osobni podaci“ također bitno za OUZP.

Primjer: U predmetu *Volker und Markus Schecke i Hartmut Eifert protiv Land Hessen*¹⁴⁸ SEU je izjavio da „u tom pogledu činjenica da se objavljeni podaci odnose na profesionalnu djelatnost nema utjecaja [...]. Europski sud za ljudska prava odlučio je u odnosu na ovu točku, u vezi s tumačenjem članka 8. Konvencije [EKLJP], da se pojam ‚privatni život‘ ne smije tumačiti restriktivno i da ne postoji načelni razlog koji bi opravdao isključivanje djelatnosti profesionalne [...] prirode iz pojma ‚privatni život‘“.

Primjer: U spojenim predmetima *Y. S. protiv Minister voor Immigratie, Integratie en Asiel* i *Minister voor Immigratie, Integratie en Asiel protiv M. i S.*¹⁴⁹ SEU je utvrdio da pravna analiza sadržana u nacrtu odluke Službe za imigraciju i naturalizaciju koja obrađuje zahtjeve za dozvolu boravka sama po sebi ne predstavlja osobne podatke, iako može sadržavati određene osobne podatke.

Sudska praksa ESLJP-a koja se odnosi na članak 8. EKLJP-a potvrđuje kako može biti teško potpuno razdvojiti pitanja iz privatnog i profesionalnog života¹⁵⁰.

147 Vidjeti ESLJP, *Amann protiv Švicarske*, br. 27798/95, 16. veljače 2000., t. 65.

148 SEU, spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010., t. 59.

149 SEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel* i *Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. srpnja 2014., t. 39.

150 Vidjeti, primjerice, ESLJP, *Rotaru protiv Rumunjske* [VV], br. 28341/95, 4. svibnja 2000., t. 43.; ESLJP, *Niemietz protiv Njemačke*, br. 13710/88, 16. prosinca 1992., t. 29.

Primjer: U predmetu *Bărbulescu protiv Rumunjske*¹⁵¹ tužitelj je otpušten jer je upotrebljavao poslodavčevu internetsku vezu tijekom radnog vremena i time prekršio interna pravila. Njegov je poslodavac nadzirao njegovu komunikaciju te su tijekom postupka pred nacionalnim sudom predloženi zapisi njegovih privatnih poruka. ESLJP je utvrdio da je članak 8. primjenjiv u ovom slučaju i ostavio je otvorenim pitanje je li na temelju ograničavajućih pravila poslodavca tužitelj mogao razumno očekivati privatnost, no u svakom je slučaju zaključio da poslodavac svojim naputcima ne može posve onemogućiti privatni društveni život na radnom mjestu. Kad je riječ o osnovanosti takva postupka, državama ugovornim strankama morao se omogućiti velik raspon procjena prilikom ocjenjivanja potrebe za uspostavljanjem pravnog okvira kojim se reguliraju uvjeti u kojima poslodavac može kontrolirati neposlovnu komunikaciju zaposlenika na radnom mjestu, bilo elektroničku ili drugu. Unatoč tome, nacionalna tijela morala su osigurati da je poslodavčevo uvođenje mjera za nadziranje dopisivanja i drugih komunikacija, neovisno o opsegu i trajanju takvih mjera, popraćeno odgovarajućim i dostatnim zaštitnim mjerama protiv zlorabe. Proporcionalnost i postupovna jamstva protiv proizvoljnog postupanja bili su od ključne važnosti, a ESLJP je utvrdio niz čimbenika koji su bili relevantni u tim okolnostima. Primjerice, takvi su čimbenici uključivali mjeru u kojoj poslodavac nadzire zaposlenike, razinu zadiranja u privatnost zaposlenika, posljedice za zaposlenika i postojanje odgovarajućih zaštitnih mjera. Usto, nacionalna tijela morala su osigurati da zaposlenik čije se komunikacije nadziru ima pristup pravnom lijeku pred pravosudnim tijelom s nadležnošću da utvrdi, barem u suštini, kako se ti navedeni kriteriji poštuju i jesu li sporne mjere zakonite. U ovom slučaju ESLJP je utvrdio da je došlo do kršenja članka 8. jer nacionalna tijela nisu omogućila odgovarajuću zaštitu prava tužitelja na poštovanje njegova privatnog života i dopisivanje, te stoga nisu uspostavila pravednu ravnotežu između predmetnih interesa.

Na temelju prava EU-a, kao i prava Vijeća Europe, informacije sadržavaju podatke o osobi:

- ako se pojedinac identificira ili ga je moguće identificirati na temelju tih informacija, ili
- ako se pojedinac, unatoč tome što nije identificiran, može selektirati na temelju tih informacija na način koji omogućuje otkrivanje ispitanika dodatnim istraživanjem.

¹⁵¹ ESLJP, *Bărbulescu protiv Rumunjske* [VV], br. 61496/08, 5. rujna 2017., t. 121.

Obje su vrste informacija na isti način zaštićene europskim zakonodavstvom o zaštiti podataka. Mogućnost izravne ili neizravne identifikacije zahtijeva neprekidnu procjenu, „uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj”¹⁵². Europski sud za ljudska prava često je ponavljao da je pojam „osobnih podataka” prema EKLJP-u isti kao u Konvenciji br. 108, osobito što se tiče uvjeta koji se odnosi na identificirane osobe ili osobe koje je moguće identificirati¹⁵³.

OUZP-om se utvrđuje da se pojedincu identitet može utvrditi kada se on „može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca”¹⁵⁴. Identifikacija stoga podrazumijeva elemente koji osobu opisuju tako da se razlikuje od svih drugih osoba i prepoznaje kao pojedinac. Ime osobe prvi je primjer takvih elemenata opisa i omogućuje izravnu identifikaciju osobe. U nekim slučajevima druge informacije mogu imati sličan učinak kao ime i omogućiti neizravnu identifikaciju osobe. Telefonski broj, broj socijalnog osiguranja i registracijski broj vozila primjeri su informacija prema kojima je pojedinca moguće identificirati. Informacije kao što su računalne datoteke, „kolačići” i alati za nadzor mrežnog prometa mogu se upotrijebiti i za selekciju pojedinaca identificiranjem njihova ponašanja i navika. Kako je objašnjeno u mišljenju Radne skupine iz članka 29., „[č]ak i bez upita o imenu i adresi pojedinca moguće ga je kategorizirati na temelju socioekonomskih, psiholoških, filozofskih i drugih kriterija ili pripisati mu određene odluke budući da za kontaktnu točku (računalo) pojedinca više nije potrebno otkrivanje njegova identiteta u užem smislu”¹⁵⁵. Definicija osobnih podataka i prema pravu Vijeća Europe i pravu EU-a dovoljno je široka da obuhvaća sve mogućnosti identifikacije (i stoga i sve stupnjeve identifikacije).

Primjer: U predmetu *Promusicae protiv Telefónica de España*¹⁵⁶ SEU je izjavio da je „neosporno da dostavljanje imena i adresa pojedinih korisnika [određene internetske platforme za zajedničko korištenje datoteka] koje je zatražila organizacija Promusicae uključuje stavljanje na raspolaganje osobnih podataka, odnosno informacija koje se tiču identificiranih fizičkih osoba ili

152 Opća uredba o zaštiti podataka, uvodna izjava 26.

153 Vidjeti ESLJP, *Amann protiv Švicarske* [VV], br. 27798/95, 16. veljače 2000., t. 65.

154 Opća uredba o zaštiti podataka, članak 4. stavak 1.

155 Radna skupina iz članka 29., *Opinion 4/2007 on the concept of personal data* (Mišljenje 4/2007 o konceptu osobnih podataka), WP 136, 20. lipnja 2007., str. 15.

156 SEU, C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. siječnja 2008., t. 45.

fizičkih osoba koje je moguće identificirati, u skladu s definicijom iz članka 2. točke (a) Direktive 95/46 [trenutačno članak 4. stavak 1. OUZP-a]. Takvo dostavljanje informacija koje je, kako je iznijela Promusicae, a Telefónica nije osporila, Telefónica pohranila, predstavlja obradu osobnih podataka”¹⁵⁷.

Primjer: Predmet *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*¹⁵⁸ odnosio se na odbijanje pružatelja internetskih usluga Scarlet da instalira sustav za filtriranje elektroničkih komunikacija koje se služe softverom za zajedničko korištenje datotekama kako bi se spriječilo zajedničko korištenje datotekama kojima se krše autorska prava koja štiti SABAM, upravljačko društvo koje zastupa književnike, skladatelje i urednike. SEU je utvrdio da su IP adrese „zaštićeni osobni podaci jer omogućuju identifikaciju korisnika”.

Budući da mnoga imena nisu jedinstvena, za utvrđivanje identiteta osobe mogu biti potrebne dodatne informacije kako bi se osiguralo da se osoba ne zamijeni s nekom drugom. Ponekad se izravne i neizravne informacije moraju kombinirati kako bi se identificirao pojedinac na kojega se informacije odnose. Često se upotrebljavaju datum i mjesto rođenja. U pojedinim su zemljama također uvedeni personalizirani brojevi kako bi se građani bolje međusobno razlikovali. Preneseni porezni podaci¹⁵⁹, podaci koji se odnose na podnositelja zahtjeva za dozvolu boravka sadržani u administrativnom dokumentu¹⁶⁰ i dokumenti koji se odnose na bankarske i fiducijarne odnose¹⁶¹ mogu predstavljati osobne podatke. Biometrijski podaci, kao što su otisci prstiju, digitalne fotografije ili skeniranje šarenice oka, podaci o lokaciji i mrežne informacije sve su važniji za identificiranje osoba u tehnološko doba.

Međutim, preduvjet za primjenjivost europskog zakonodavstva o zaštiti podataka nije stvarna identifikacija ispitanika. Dovoljno je da se dotična osoba može identificirati. Smatra se da se osoba može identificirati ako je dostupno dovoljno elemenata

157 Nekadašnja Direktiva 95/46/EZ, članak 2. točka (b), sada Opća uredba o zaštiti podataka, članak 4. stavak 2.

158 SEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. studenoga 2011., t. 51.

159 SEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. listopada 2015.

160 SEU, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. srpnja 2014.

161 ESJP, *M. N. i drugi protiv San Marina*, br. 28005/12, 7. srpnja 2015.

na temelju kojih se osoba može izravno ili neizravno identificirati¹⁶². Sukladno uvodnoj izjavi 26. OUZP-a, to se procjenjuje na temelju vjerojatnosti da će predvidivim korisnicima informacija biti dostupni prihvatljivi instrumenti identifikacije i da će ih korisnici primijeniti, što uključuje informacije koje posjeduju primatelji treće strane (vidjeti dio 2.3.2.).

Primjer: Lokalno tijelo odluči prikupljati podatke o vozilima koja prebrzo prometuju lokalnim cestama. Potom fotografira vozila, automatski snimajući vrijeme i lokaciju, kako bi te podatke proslijedilo nadležnom tijelu radi kažnjavanja prijestupnika. Ispitanik ulaže žalbu tvrdeći da lokalno tijelo, sukladno zakonodavstvu o zaštiti podataka, nema pravne osnove za takvo prikupljanje podataka. Lokalno tijelo smatra da ne prikuplja osobne podatke tvrdeći da su podaci o registraciji anonimni. Lokalno tijelo nema pravnu ovlast pristupa općem registru vozila za otkrivanje identiteta vlasnika vozila ili vozača.

Taj se argument ne podudara s uvodnom izjavom 26. OUZP-a. S obzirom na to da je očita svrha prikupljanja podataka identificirati i kazniti prekršitelje, izgledno je da će se pokušati izvršiti identifikacija. Premda lokalna tijela nemaju izravan pristup sredstvima identifikacije, ona će podatke proslijediti nadležnom tijelu, odnosno policiji, koja raspolaže tim sredstvima. Iz uvodne izjave 26. također jasno proizlazi scenarij prema kojemu se može predvidjeti da daljnji primatelji podataka, osim neposrednog korisnika podataka, mogu pokušati identificirati pojedinca. U kontekstu uvodne izjave 26., radnja koju je poduzelo lokalno tijelo izjednačena je s prikupljanjem podataka o osobama koje se mogu identificirati, te je stoga za nju, sukladno zakonodavstvu o zaštiti podataka, potrebna pravna osnova.

„Kako bi se utvrdilo je li po svemu sudeći izgledno da se upotrebljavaju sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i tehnologiju dostupnu u vrijeme obrade i tehnološki razvoj”¹⁶³.

¹⁶² Opća uredba o zaštiti podataka, članak 4. stavak 1.

¹⁶³ *Ibid.*, uvodna izjava 26.

Primjer: U predmetu *Breyer protiv Bundesrepublik Deutschland*¹⁶⁴ SEU je razmatrao koncept moguće neizravne identifikacije ispitanika. Predmet se odnosio na dinamičke IP adrese, koje se mijenjaju svaki put kada se uspostavi nova veza s internetom. Internetske stranice kojima upravljaju savezne njemačke institucije registrirale su i pohranjivale dinamičke IP adrese kako bi se spriječili kibernetički napadi i po potrebi pokrenuli kazneni postupci. Samo je pružatelj internetskih usluga kojim se služio g. Breyer imao dodatne informacije potrebne za njegovu identifikaciju.

SEU je smatrao da dinamička IP adresa, koju pružatelj usluga elektroničkih medija registrira kada korisnik pristupi internetskoj stranici koju je pružatelj stavio na raspolaganje javnosti, predstavlja osobne podatke samo ako treća strana, odnosno pružatelj internetskih usluga u ovom slučaju, ima dodatne podatke potrebne za identifikaciju te osobe¹⁶⁵. Tvrdio je da „nije potrebno da se sve informacije koje omogućuju identifikaciju osobe o kojoj je riječ moraju nalaziti u posjedu samo jedne osobe” da bi se informacije mogle kvalificirati kao osobni podaci. Korisnici dinamičkih IP adresa koje registrira pružatelj internetskih usluga mogu se identificirati u određenim situacijama, primjerice u okviru kaznenog postupka u slučaju kibernetičkih napada, uz pomoć drugih osoba¹⁶⁶. Prema SEU-u, ako pružatelj usluga „raspolaze pravnim sredstvima koji mu omogućuju identifikaciju navedene osobe pomoću dodatnih informacija kojima raspolaze pružatelj internetskog pristupa te osobe”, to predstavlja „sredstvo koje se može opravdano koristiti za utvrđivanje navedene osobe”. Stoga se takvi podaci smatraju osobnim podacima.

Na temelju prava Vijeća Europe mogućnost identifikacije tumači se na sličan način. Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108 sadržava sličan opis: koncept „mogućnosti identificiranja” ne odnosi se samo na građanski ili pravni identitet pojedinca nego i na sve što može omogućiti „individualizaciju” odnosno selekciju pojedinca u odnosu na druge, a stoga i potencijalno drugačije postupanje prema njemu. Ta se „individualizacija” može izvesti, primjerice, posebnim upućivanjem na tu osobu ili na uređaj ili kombinaciju uređaja (računalo, mobilni telefon, kamera,

164 SEU, C-582/14, *Patrick Breyer protiv Bundesrepublik Deutschland*, 19. listopada 2016., t. od 47. do 48.

165 Nekadašnja Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, članak 2. točka (a).

166 SEU, C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. studenoga 2011., t. 47. i 48.

igraće konzole itd.) koji su povezani s identifikacijskim brojem, pseudonimom, biometrijskim ili genetskim podacima, podacima o lokaciji, IP adresom ili drugim identifikatorom¹⁶⁷. Ne smatra se da se pojedinca „može identificirati” ako je za njegovu identifikaciju potrebno neuobičajeno mnogo vremena, truda i resursa. To je slučaj, primjerice, kada bi za identificiranje ispitanika bile potrebne prekomjerno složene, duge i skupocjene radnje. Nerazumnost utrošenog vremena, truda i resursa mora se procijeniti za svaki pojedini slučaj, uzimajući u obzir čimbenike poput svrhe obrade, cijene i koristi identifikacije, vrste voditelja obrade i primijenjene tehnologije¹⁶⁸.

Važno je napomenuti da oblik u kojem se osobni podaci pohranjuju ili upotrebljavaju nije relevantan za primjenjivost zakonodavstva o zaštiti podataka. Pismena ili usmena komunikacija može sadržavati osobne podatke, kao i slike¹⁶⁹, uključujući snimku¹⁷⁰ ili zvuk¹⁷¹ televizije zatvorenog kruga (CCTV). Elektronički snimljene informacije, kao i informacije na papiru, također mogu biti osobni podaci. Čak i stanični uzorci ljudskog tkiva, u kojima se bilježi DNK pojedinca, mogu biti izvori iz kojih se mogu izdvojiti biometrijski podaci¹⁷² ako se ti podaci odnose na naslijeđena ili stečena genetska obilježja pojedinca, ako pružaju jedinstvene informacije o njegovu zdravlju ili fiziologiji te ako proizlaze iz analize biološkog uzorka te osobe¹⁷³.

Anonimizacija

Sukladno načelu ograničenog čuvanja podataka sadržanom u Općoj uredbi o zaštiti podataka te moderniziranoj Konvenciji br. 108 (o kojem se detaljnije raspravlja u poglavlju 3.), podaci se moraju čuvati „u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci

167 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 18.

168 *Ibid.*, t. 17.

169 ESLJP, *Von Hannover protiv Njemačke*, br. 59320/00, 24. lipnja 2004.; ESLJP, *Sciaccia protiv Italije*, br. 50774/99, 11. siječnja 2005.; SEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. prosinca 2014.

170 ESLJP, *Peck protiv Ujedinjene Kraljevine*, br. 44647/98, 28. siječnja 2003.; ESLJP, *Köpke protiv Njemačke* (odl.), br. 420/07, 5. listopada 2010.; EDPS (2010.), *The EDPS video-surveillance guidelines* (Smjernice EDPS-a o videonadzoru), 17. ožujka 2010.

171 ESLJP, *P. G. i J. H. protiv Ujedinjene Kraljevine*, br. 44787/98, 25. rujna 2001, t. 59. i 60.; ESLJP, *Wisse protiv Francuske*, br. 71611/01, 20. prosinca 2005. (inačica na francuskom jeziku).

172 Vidjeti Radna skupina iz članka 29. (2007.), *Mišljenje 4/2007 o konceptu osobnih podataka*, WP136, 20. lipnja 2007., str. 9.; Vijeće Europe, Recommendation No. Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin (Preporuka br. Rec(2006)4 Odbora ministara državama članicama o istraživanju bioloških materijala ljudskog podrijetla), 15. ožujka 2006.

173 Opća uredba o zaštiti podataka, članak 4. stavak 13.

obrađuju¹⁷⁴. Sukladno tome, kada podaci više nisu potrebni i ne služe prvobitnoj svrsi, moraju se izbrisati ili anonimizirati ako ih voditelj obrade želi pohraniti.

Postupak anonimizacije podataka podrazumijeva da su svi elementi identifikacije uklonjeni iz skupa osobnih podataka kako se ispitanik više ne bi mogao identificirati¹⁷⁵. Radna skupina iz članka 29. u svojem Mišljenju 05/2014 analizira učinkovitost i ograničenja različitih tehnika anonimizacije¹⁷⁶. Potvrđuje potencijalnu vrijednost takvih tehnika, no naglašava da određene tehnike nisu nužno primjenjive u svim slučajevima. Da bi se pronašlo optimalno rješenje u određenoj situaciji, odgovarajući postupak anonimizacije treba se odrediti za svaki pojedini slučaj. Neovisno o tehnici koja se primjenjuje, identifikacija se mora spriječiti, i to nepovratno. To znači da, kako bi podaci bili anonimizirani, u informacijama ne smije biti prisutan nijedan element koji bi uz primjenu razumnog truda mogao poslužiti za ponovnu identifikaciju dotične osobe (ili osoba)¹⁷⁷. Rizik od ponovne identifikacije može se procijeniti uzimajući u obzir „vrijeme, trud ili resurse potrebne s obzirom na prirodu podataka, kontekst njihove upotrebe, dostupne tehnologije za ponovnu identifikaciju i povezane troškove”¹⁷⁸.

Kada su podaci uspješno anonimizirani, više nisu osobni i zakonodavstvo o zaštiti podataka više se ne primjenjuje.

OUZP-om se propisuje da se osoba ili organizacija koja nadzire obradu osobnih podataka ne može obvezati na čuvanje, prikupljanje ili obradu dodatnih podataka za identifikaciju ispitanika isključivo radi usklađivanja s Uredbom. Međutim, to pravilo ima značajnu iznimku: kad god ispitanik pruži dodatne informacije voditelju obrade koje omogućuju njegovu identifikaciju radi ostvarivanja prava na pristup osobnim podacima, ispravak ili brisanje podataka, ograničavanje obrade i prenosivost podataka, podaci koji su prethodno anonimizirani ponovno postaju osobni podaci¹⁷⁹.

174 *Ibid.*, članak 5. stavak 1. točka (e); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (e).

175 Opća uredba o zaštiti podataka, uvodna izjava 26.

176 Radna skupina iz članka 29. (2014.), *Opinion 05/2014 on Anonymization Techniques* (Mišljenje 05/2014 o tehnikama anonimizacije), WP 216, 10. travnja 2014.

177 Opća uredba o zaštiti podataka, uvodna izjava 26.

178 Vijeće Europe, Odbor za Konvenciju br. 108 (2017.), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka), 23. siječnja 2017., t. 6.2.

179 Opća uredba o zaštiti podataka, članak 11.

Pseudonimizacija

Osobni podaci sadržavaju informacije poput imena, datuma rođenja, spola i adrese ili druge elemente koji mogu dovesti do identifikacije. Postupak pseudonimizacije osobnih podataka podrazumijeva zamjenu tih informacija pseudonimom.

U **pravu EU-a** „pseudonimizacija” se definira kao „obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi”¹⁸⁰. Za razliku od anonimiziranih podataka, pseudonimizirani podaci i dalje su osobni podaci, i stoga podliježu zakonodavstvu o zaštiti podataka. Iako se pseudonimizacijom mogu smanjiti sigurnosni rizici za ispitanike, ona nije izuzeta iz područja primjene OUZP-a.

U OUZP-u su različite primjene pseudonimizacije prepoznate kao primjerene tehničke mjere za poboljšanje zaštite podataka, a posebno se navodi za oblik i sigurnost obrade podataka¹⁸¹. To je također primjerena zaštitna mjera koja se može upotrijebiti za obradu osobnih podataka u svrhe za koje nisu prvotno prikupljeni¹⁸².

Pseudonimizacija se ne spominje izričito u pravnim definicijama modernizirane Konvencije br. 108 **Vijeća Europe**. Međutim, u Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 jasno se navodi da „upotreba pseudonima ili bilo kojeg digitalnog identifikatora / digitalnog identiteta ne dovodi do anonimizacije podataka jer se ispitanika i dalje može identificirati ili individualizirati”¹⁸³. Jedan od načina na koji se podaci mogu pseudonimizirati jest šifriranje podataka. Nakon pseudonimizacije podataka poveznica s identitetom postoji u obliku pseudonima uz ključ za dešifriranje. Bez tog ključa teško je identificirati pseudonimizirane podatke. Međutim, oni koji su ovlašteni upotrebljavati takav ključ mogu ponovno jednostavno identificirati osobu. Posebno valja spriječiti da neovlaštene osobe upotrebljavaju ključeve za dešifriranje. Stoga se „[p]seudonimni podaci [...] smatraju osobnim podacima [...]” obuhvaćenima moderniziranom Konvencijom br. 108¹⁸⁴.

180 *Ibid.*, članak 4. stavak 5.

181 *Ibid.*, članak 25. stavak 1.

182 *Ibid.*, članak 6. stavak 4.

183 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 18.

184 *Ibid.*

Autentifikacija

Autentifikacija je postupak u kojem osoba može dokazati da posjeduje određeni identitet i/ili da je ovlaštena za određene radnje, poput pristupanja sigurnosnim područjima ili podizanja novca s bankovnog računa. Autentifikacija se može provesti: usporedbom biometrijskih podataka, kao što je fotografija ili otisak prsta u putovnici, s podacima kojima se osoba predstavlja prilikom, na primjer, imigracijske kontrole¹⁸⁵; ili traženjem podataka koje bi trebala znati samo osoba određenog identiteta ili s određenom ovlašću, kao što je jedinstveni identifikacijski broj (PIN) ili lozinka; ili traženjem da se predoči određeni token koji bi trebao biti u isključivom posjedu osobe određenog identiteta ili s određenom ovlašću, kao što su posebna čip-kartica ili ključ bankovnog sefa. Osim lozinki ili čip-kartica, elektronički potpis, katkad zajedno s PIN-ovima, vrlo je učinkovit instrument identifikacije i autentifikacije osobe u elektroničkim komunikacijama.

2.1.2. Posebne kategorije osobnih podataka

Na temelju prava EU-a, kao i **prava Vijeća Europe**, postoje posebne kategorije osobnih podataka koji zbog svoje prirode prilikom obrade mogu predstavljati rizik za ispitanike, te ih stoga treba dodatno zaštititi. Takvi podaci podliježu načelu zabrane i uvjeti u kojima je takva obrada zakonita jesu ograničeni.

U okviru modernizirane Konvencije br. 108 (članak 6.) i OUZP-a (članak 9.) sljedeće se kategorije smatraju osjetljivim podacima:

- osobni podaci kojima se otkriva rasno ili etničko podrijetlo,
- osobni podaci kojima se otkrivaju politička mišljenja, vjerska ili druga uvjerenja, uključujući filozofske stavove,
- osobni podaci kojima se otkriva članstvo u sindikatima,
- genetski i biometrijski podaci koji se obrađuju u svrhu identifikacije osobe,
- osobni podaci u vezi sa zdravljem, spolnim životom ili seksualnom orijentacijom.

185 *Ibid.*, t. 56. i 57.

Primjer: Predmet *Bodil Lindqvist*¹⁸⁶ odnosio se na upućivanje na različite osobe na internetskoj stranici navođenjem njihova imena ili na druge načine, primjerice navođenjem njihova telefonskog broja ili informacija o njihovim hobijima. SEU je izjavio da „pozivanje na činjenicu da je osoba ozlijedila stopalo, a zaposlena je na nepuno radno vrijeme, iz medicinskih razloga predstavlja osobne podatke koji se tiču zdravlja”¹⁸⁷.

Osobni podaci povezani s kaznenim djelima i osudama

U moderniziranoj Konvenciji br. 108 navode se osobni podaci koji se odnose na kaznena djela, kaznene postupke i osude te s njima povezane sigurnosne mjere u sklopu popisa posebnih kategorija osobnih podataka¹⁸⁸. U okviru OUZP-a osobni podaci koji se odnose na kaznena djela, kaznene postupke i osude te s njima povezane sigurnosne mjere ne spominju se u sklopu popisa posebnih kategorija podataka, ali se obrađuju u zasebnom članku. U članku 10. OUZP-a utvrđuje se da se obrada takvih podataka može provoditi samo „pod nadzorom službenog tijela ili kada je obrada odobrena pravom Unije ili pravom države članice kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode ispitanikâ”. S druge strane, sveobuhvatni registri podataka o kaznenim osudama mogu se voditi pod nadzorom određenih službenih tijela¹⁸⁹. Obrada osobnih podataka u kontekstu izvršavanja zakonodavstva u EU-u se regulira posebnim pravnim instrumentom, Direktivom (EU) 2016/680¹⁹⁰. Direktivom se utvrđuju posebna pravila zaštite podataka, koja su obvezujuća za nadležna tijela kada obrađuju osobne podatke u svrhu sprečavanja, istrage, otkrivanja i progona kaznenih djela (vidjeti [dio 8.2.1.](#)).

186 SEU, C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003., t. 51.

187 Nekadašnja Direktiva 95/46/EZ, članak 8. točka (1), sada Opća uredba o zaštiti podataka, članak 9. stavak 1.

188 Modernizirana Konvencija br. 108, članak 6. stavak 1.

189 Opća uredba o zaštiti podataka, članak 10.

190 Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL 2016 L 119.

2.2. Obrada podataka

Ključne točke

- „Obrada podataka” odnosi se na svaku radnju koja se obavlja nad osobnim podacima.
- Pojam „obrada” obuhvaća automatiziranu i neautomatiziranu obradu.
- Prema pravu EU-a „obrada” se odnosi i na ručnu obradu u strukturiranim sustavima arhiviranja.
- Prema pravu Vijeća Europe značenje „obrade” može se proširiti u okviru nacionalnog zakonodavstva kako bi obuhvatilo ručnu obradu.

2.2.1. Koncept obrade podataka

Koncept obrade osobnih podataka sveobuhvatno je definiran **i u pravu EU-a i u pravu Vijeća Europe**: „„obrada osobnih podataka’ [...] znači svaki postupak ili skup postupaka [...] kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje”¹⁹¹ osobnih podataka. U moderniziranoj Konvenciji br. 108 definiciji se dodaje čuvanje osobnih podataka¹⁹².

Primjer: U predmetu *František Ryneš*¹⁹³ g. Ryneš snimio je sliku dviju osoba koje su razbile prozore na njegovu domu, s pomoću kućnog sustava videonadzora s televizijom zatvorenog kruga (CCTV) koji je postavio radi zaštite svoje imovine. SEU je utvrdio da videonadzor koji uključuje snimanje i pohranu osobnih podataka predstavlja automatsku obradu podataka, koja je obuhvaćena područjem primjene zakonodavstva EU-a o zaštiti podataka.

191 Opća uredba o zaštiti podataka, članak 4. stavak 2. Vidjeti i moderniziranu Konvenciju br. 108, članak 2. točka (b).

192 Modernizirana Konvencija br. 108, članak 2. točka (b).

193 SEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. prosinca 2014., t. 25.

Primjer: U predmetu *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*¹⁹⁴ g. Manni zatražio je uklanjanje svojih osobnih podataka iz registra za rejting trgovačkih društava koji su ga povezivali s likvidacijom društva za poslovanje nekretninama te tako negativno utjecali na njegov ugled. SEU je smatrao da „upisivanjem i čuvanjem navedenih podataka u registru i njihovom dostavom, prema potrebi, na zahtjev trećih [osoba], tijelo zaduženo za vođenje tog registra provodi „obradu osobnih podataka“ za koju je „odgovorno““.

Primjer: Poslodavci prikupljaju i obrađuju podatke o svojim zaposlenicima, uključujući informacije o njihovim plaćama. Pravna osnova za zakonitost tog čina jest ugovor o radu.

Poslodavci podatke o plaćama zaposlenika prosljeđuju poreznim tijelima. Takvo se prosljeđivanje podataka također smatra „obradom“ u smislu značenja tog pojma u moderniziranoj Konvenciji br. 108 i OUZP-u. Međutim, pravna osnova za takvo otkrivanje podataka nije ugovor o radu. Mora postojati dodatna pravna osnova za postupke obrade koji podrazumijevaju prijenos podataka o plaćama od poslodavca do poreznog tijela. Ta je pravna osnova obično sadržana u odredbama nacionalnih poreznih zakona. Bez takvih odredbi, i bez neke druge legitimne osnove za obradu, takav prijenos podataka smatrao bi se nezakonitom obradom.

2.2.2. Automatizirana obrada podataka

Zaštita podataka na temelju modernizirane Konvencije br. 108 i OUZP-a u potpunosti se primjenjuje na automatiziranu obradu podataka.

Na temelju **prava EU-a**, automatizirana obrada podataka odnosi se na radnje izvršene nad osobnim podacima djelomično ili u cijelosti automatiziranim sredstvima¹⁹⁵. Modernizirana Konvencija br. 108 sadržava sličnu definiciju¹⁹⁶. U praktičnom smislu to znači da je svaka obrada osobnih podataka automatiziranim sredstvima

¹⁹⁴ SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. ožujka 2017., t. 35.

¹⁹⁵ Opća uredba o zaštiti podataka, članak 2. stavak 1. i članak 4. stavak 2.

¹⁹⁶ Modernizirana Konvencija br. 108, članak 2. točke (b) i (c); Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 21.

s pomoću, primjerice, osobnog računala, mobilnog uređaja ili usmjerivača obuhvaćena propisima o zaštiti podataka EU-a i Vijeća Europe.

Primjer: Predmet *Bodil Lindqvist*¹⁹⁷ odnosio se na upućivanje na različite osobe na internetskoj stranici navođenjem njihova imena ili na druge načine, primjerice navođenjem njihova telefonskog broja ili informacija o njihovim hobijima. SEU je zaključio da „navođenje različitih osoba na internetskoj stranici i njihovo identificiranje putem imena i prezimena ili na drugi način, primjerice navođenjem njihova telefonskog broja ili informacija u vezi s njihovim radnim uvjetima ili hobijima, predstavlja „podatke koji se u cijelosti ili djelomično obrađuju automatskim putem” u smislu članka 3. stavka 1. Direktive 95/46/EZ¹⁹⁸.

Primjer: U predmetu *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González*¹⁹⁹ g. González zatražio je uklanjanje ili izmjenu poveznice između njegova imena u internetskoj tražilici Google i dviju stranica u novinama u kojima je objavljena dražbena prodaja nekretnina radi naplate dugovanja za socijalno osiguranje. SEU je naveo da „pretražujući internet na automatiziran, stalan i sustavan način u potrazi za informacijama koje su na njemu objavljene, operater pretraživača „prikuplja” takve podatke koje zatim „vraća”, „snima” i „organizira” u okviru svojih programa indeksiranja, „pohranjuje” na svojim poslužiteljima i u određenim slučajevima „otkriva” i „stavlja na raspolaganje” svojim korisnicima rezultate njihovih pretraga u obliku popisa”²⁰⁰. SEU je zaključio da takve radnje predstavljaju „obrađu”, „a nije relevantno to da operater pretraživača iste operacije jednako primjenjuje na druge vrste informacija i to da ne razlikuje njih i osobne podatke”.

197 SEU, C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003., t. 27.

198 Opća uredba o zaštiti podataka, članak 2. stavak 1.

199 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014.

200 *Ibid.*, t. 28.

2.2.3. Neautomatizirana obrada podataka

Ručna obrada podataka također zahtijeva zaštitu podataka.

Zaštita podataka **na temelju prava EU-a** ni na koji način nije ograničena na automatiziranu obradu podataka. U skladu s tim, na temelju prava EU-a zaštita podataka primjenjuje se na obradu osobnih podataka u ručnom sustavu arhiviranja, tj. posebno strukturiranoj papirnoj datoteci²⁰¹. Strukturirani sustav arhiviranja sustav je u kojemu se kategorizira skup osobnih podataka te su oni dostupni na temelju određenih kriterija. Primjerice, ako poslodavac vodi papirnu datoteku pod nazivom „dopust zaposlenika” u kojoj su sadržane sve pojedinosti o dopustima koje je osoblje uzelo u protekloj godini i koja je organizirana prema abecednom redoslijedu, datoteka će činiti ručni sustav arhiviranja, koji podliježe propisima EU-a o zaštiti podataka. Razlog takva proširenja zaštite podataka jest to što se:

- papirne datoteke mogu strukturirati tako da omogućuju brzo i jednostavno pronalaženje informacija,
- pohranom osobnih podataka u strukturiranim papirnim datotekama lakše zaobilaze zakonski propisana ograničenja automatizirane obrade podataka²⁰².

Na temelju **prava Vijeća Europe**, u definiciji automatske obrade prepoznato je da među pojedinim automatiziranim radnjama mogu biti potrebne određene faze ručne uporabe osobnih podataka²⁰³. Člankom 2. točkom (c) modernizirane Konvencije br. 108 utvrđuje se da „[a]ko se ne upotrebljava automatizirana obrada, obrada podataka podrazumijeva radnju ili skup radnji izvršenih na osobnim podacima unutar strukturiranog skupa takvih podataka koji je dostupan ili se može pronaći sukladno određenim kriterijima”.

201 Opća uredba o zaštiti podataka, članak 2. stavak 1.

202 Opća uredba o zaštiti podataka, uvodna izjava 15.

203 Modernizirana Konvencija br. 108, članak 2. točke (b) i (c).

2.3. Korisnici osobnih podataka

Ključne točke

- Osoba koja odlučuje o načinima i svrhama obrade osobnih podataka drugih naziva se „voditelj obrade” sukladno zakonodavstvu o zaštiti podataka. Ako nekoliko osoba zajednički donosi tu odluku, one mogu biti „zajednički voditelji obrade”.
- „Izvršitelj obrade” fizička je ili pravna osoba koja obrađuje osobne podatke u ime voditelja obrade.
- Izvršitelj obrade postaje voditelj obrade ako odlučuje o načinima i svrhama same obrade podataka.
- Svaka je osoba kojoj se prenesu podaci „primatelj”.
- „Treća strana” fizička je ili pravna osoba koja nije ispitanik, voditelj obrade, izvršitelj obrade ni osoba koja je ovlaštena za obradu osobnih podataka pod izravnom nadležnošću voditelja ili izvršitelja obrade.
- Privola kao pravna osnova za obradu osobnih podataka mora biti dobrovoljno dana, utemeljena na informacijama, posebna i nedvosmislena naznaka želja potvrđena jasnim činom koji predstavlja pristajanje na obradu.
- Za obradu posebnih kategorija podataka na temelju privole potrebna je izričita privola.

2.3.1. Voditelji obrade i izvršitelji obrade

Najvažnija je posljedica obnašanja funkcije voditelja ili izvršitelja obrade pravna odgovornost za ispunjavanje odgovarajućih obveza koje proizlaze iz zakonodavstva o zaštiti podataka. U privatnom je sektoru to obično fizička ili pravna osoba, a u javnom sektoru nadležno tijelo. Postoji značajna razlika između voditelja obrade podataka i izvršitelja obrade podataka: voditelj obrade fizička je ili pravna osoba koja donosi odluke o svrhama i načinima obrade, a izvršitelj obrade fizička ili pravna osoba koja obrađuje podatke u ime voditelja obrade, pridržavajući se strogih naputaka. U načelu, voditelj obrade podataka nadzire obradu i snosi odgovornost za nju, uključujući pravnu odgovornost. Međutim, od uvođenja reformi propisa o zaštiti podataka, izvršitelji obrade imaju obvezu usklađivanja s mnoštvom zahtjeva koji se primjenjuju na voditelje obrade. Primjerice, prema OUZP-u, izvršitelji obrade moraju voditi evidenciju svih kategorija aktivnosti obrade kako bi dokazali usklađenost s obvezama koje imaju na temelju Uredbe²⁰⁴. Izvršitelji obrade također moraju

204 Opća uredba o zaštiti podataka, članak 30. stavak 2.

provesti odgovarajuće tehničke i organizacijske mjere kako bi osigurali sigurnost obrade²⁰⁵, imenovati službenika za zaštitu podataka u određenim slučajevima²⁰⁶ te obavijestiti voditelja obrade o povredama podataka²⁰⁷.

Hoće li osoba moći odrediti i utvrditi svrhu i načine obrade, ovisit će o činjenicama ili okolnostima pojedinog slučaja. Prema definiciji voditelja obrade iz OUZP-a, tu funkciju mogu obavljati fizičke osobe, pravne osobe ili bilo koja druga tijela. Međutim, Radna skupina iz članka 29. naglasila je kako bi se, da bi se pojedincima pružio stabilniji subjekt putem kojega mogu ostvariti svoja prava, „za funkciju voditelja obrade trebalo razmatrati društvo ili tijelo kao takvo umjesto određene osobe unutar društva ili tijela”²⁰⁸. Primjerice, društvo koje prodaje medicinske potrepštine liječnicima voditelj je obrade za sastavljanje i vođenje popisa za distribuciju koji sadržava sve liječnike na određenom području, a ne voditelj prodaje koji doista upotrebljava i vodi popis.

Primjer: Kad marketinški odjel društva Sunshine planira obrađivati podatke u svrhe istraživanja tržišta, onda je voditelj obrade društvo Sunshine, a ne zaposlenici marketinškog odjela. Marketinški odjel ne može biti voditelj obrade jer nema zasebnu pravnu osobnost.

Fizičke osobe mogu biti voditelji obrade i prema pravu Unije i prema pravu Vijeća Europe. Međutim, prilikom obrade podataka o drugim osobama koji se odnose na isključivo osobnu ili kućnu aktivnost, pojedinci ne potpadaju pod pravila iz OUZP-a i modernizirane Konvencije br. 108 te se ne smatraju voditeljima obrade²⁰⁹. Pojedinaac koji čuva zapise o svojem dopisivanju, vodi osobni dnevnik u kojemu opisuje događaje koji uključuju prijatelje i suradnike te evidenciju o zdravstvenom stanju članova obitelji može biti izuzet od propisa o zaštiti podataka jer te aktivnosti mogu biti isključivo osobne ili kućne. U OUZP-u se dodatno utvrđuje da osobne ili kućne aktivnosti također mogu uključivati socijalno umrežavanje i internetske aktivnosti

²⁰⁵ *Ibid.*, članak 32.

²⁰⁶ *Ibid.*, članak 37.

²⁰⁷ *Ibid.*, članak 33. stavak 2.

²⁰⁸ Radna skupina iz članka 29. (2010.), *Opinion 1/2010 on the concepts of „controller” and „processor”* (Mišljenje 1/2010 o pojmovima „voditelj obrade” i „izvršitelj obrade”), WP 169, Bruxelles, 16. veljače 2010.

²⁰⁹ Opća uredba o zaštiti podataka, uvodna izjava 18. i članak 2. stavak 2. točka (c); modernizirana Konvencija br. 108, članak 3. točka (2).

poduzete u kontekstu takvih aktivnosti²¹⁰. S druge strane, propisi o zaštiti podataka u potpunosti se primjenjuju na voditelje obrade i izvršitelje obrade koji pružaju sredstva za obradu osobnih podataka za osobne ili kućne aktivnosti (primjerice, platforme društvenih mreža)²¹¹.

Pristup građana internetu i njihova mogućnost upotrebe platformi za e-trgovinu, društvenih mreža i internetskih stranica s blogovima za dijeljenje osobnih podataka o sebi i drugim osobama sve više otežavaju razdvajanje osobne od neosobne obrade²¹². Jesu li aktivnosti isključivo osobne ili kućne, ovisi o okolnostima²¹³. Aktivnosti koje imaju profesionalne ili komercijalne aspekte ne mogu biti izuzete kao kućne aktivnosti²¹⁴. Stoga kada opseg i učestalost obrade podataka ukazuju na profesionalnu aktivnost ili aktivnost na puno radno vrijeme, pojedinac se može smatrati voditeljem obrade. Uz profesionalna ili komercijalna obilježja aktivnosti obrade, dodatan čimbenik koji se mora uzeti u obzir jest dostupnost osobnih podataka velikom broju ljudi izvan privatne sfere pojedinca. Na temelju sudske prakse u okviru Direktive o zaštiti podataka, zakonodavstvo o zaštiti podataka primjenjuje se kada pojedinac prilikom upotrebe interneta objavljuje podatke o drugima na javnoj internetskoj stranici. SEU još nije donosio presude o sličnim činjenicama na temelju OUZP-a, koji pruža više smjernica o temama za koje se može smatrati da izlaze iz okvira područja primjene zakonodavstva o zaštiti podataka u sklopu „izuzeća za kućanske aktivnosti“, poput upotrebe društvenih mreža u osobne svrhe.

Primjer: Predmet *Bodil Lindqvist*²¹⁵ odnosio se na upućivanje na različite osobe na internetskoj stranici navođenjem njihova imena ili na druge načine, primjerice navođenjem njihova telefonskog broja ili informacija o njihovim hobijima. SEU je zaključio da „navođenje različitih osoba na internetskoj stranici i njihovo identificiranje putem imena i prezimena ili na drugi način [...] predstavlja „podatke koji se u cijelosti ili djelomično obrađuju automatskim putem“ u smislu članka 3. stavka 1. Direktive o zaštiti podataka²¹⁶.

210 Opća uredba o zaštiti podataka, uvodna izjava 18.

211 *Ibid.*, uvodna izjava 18.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 29.

212 Vidjeti izjavu Radne skupine iz članka 29. o raspravama o paketu reformi za zaštitu podataka (2013.), *Annex 2 : Proposals and Amendments regarding exemption for personal or household activities* (Prilog 2.: Prijedlozi i izmjene u pogledu izuzeća za osobne ili kućne aktivnosti), 27. veljače 2013.

213 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 28.

214 Vidjeti Opću uredbu o zaštiti podataka, uvodna izjava 18. i Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 27.

215 SEU, C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003.

216 *Ibid.*, t. 27.; nekadašnja Direktiva 95/46/EZ, članak 3. točka (1), sada Opća uredba o zaštiti podataka, članak 2. stavak 1.

Takva obrada osobnih podataka ne spada u aktivnosti isključivo osobne ili kućne naravi, koje su izvan područja primjene propisa EU-a o zaštiti podataka, jer se takva iznimka „valja tumačiti kao da se odnosi isključivo na aktivnosti koje su dio privatnog ili obiteljskog života pojedinaca, što očito nije slučaj s obradom osobnih podataka koja podrazumijeva njihovu objavu na internetu na način da se pristup tim podacima omogući neodređenom broju osoba”²¹⁷.

Prema SEU-u, vizualne snimke snimljene privatno postavljenom sigurnosnom kamerom u određenim okolnostima također mogu biti obuhvaćene zakonodavstvom EU-a o zaštiti podataka.

Primjer: U predmetu *František Ryneš*²¹⁸ g. Ryneš snimio je sliku dviju osoba koje su razbile prozore na njegovu domu, s pomoću kućnog sustava video-nadzora s televizijom zatvorenog kruga (CCTV) koji je postavio radi zaštite svoje imovine. Snimka je zatim predana policiji i upotrijebljena u kaznenom postupku.

SEU je izjavio da „[u] mjeri u kojoj videonadzor [...] obuhvaća, iako djelomično, javni prostor, te je zbog te činjenice usmjeren prema eksterijeru privatne sfere onoga tko provodi obradu podataka tim sredstvom, ta se obrada ne može smatrati isključivo ‚osobnom ili domaćom‘ aktivnošću [...]”²¹⁹.

Voditelj obrade

U pravu EU-a voditelj obrade definira se kao netko tko „sam ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka”²²⁰. Odlukom voditelja obrade utvrđuje se zašto se i kako podaci obrađuju.

U pravu Vijeća Europe, u moderniziranoj Konvenciji br. 108 „voditelj obrade” definira se kao „fizička ili pravna osoba, javno tijelo, služba, agencija ili bilo koje drugo tijelo koje samo ili zajedno s drugima ima ovlast donošenja odluka o obradi podataka”²²¹. Takva se ovlast donošenja odluka odnosi na svrhe i načine obrade, kao i na

217 SEU, C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003., t. 47.

218 SEU, C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. prosinca 2014., t. 33.

219 Nekadašnja Direktiva 95/46/EZ, članak 3. stavak 2. druga alineja, sada Opća uredba o zaštiti podataka, članak 2. stavak 2. točka (c).

220 Opća uredba o zaštiti podataka, članak 4. stavak 7.

221 Modernizirana Konvencija br. 108, članak 2. točka (d).

kategorije podataka koji se obrađuju te pristup podacima²²². Temelji li se ta ovlast na zakonitom imenovanju ili činjeničnim okolnostima, mora se odlučiti u svakom pojedinom slučaju²²³.

Primjer: Predmet *Google Spain*²²⁴ pokrenuo je građanin Španjolske koji je htio da se stari novinski izvještaj o njegovoj financijskoj prošlosti ukloni iz tražilice Google.

SEU je trebao odlučiti je li društvo Google kao operater internetske tražilice „voditelj obrade” podataka u smislu članka 2. točke (d) Direktive o zaštiti podataka²²⁵. SEU je smatrao da se širokom definicijom pojma „voditelja obrade” osigurava „učinkovitu i potpunu zaštitu osoba čiji se podaci obrađuju”²²⁶. SEU je zaključio da operater internetske tražilice određuje svrhe i načine te aktivnosti, kao i to da podatke koje na internetske stranice učita-vaju izdavači internetskih stranica stavlja na raspolaganje svakom korisniku interneta koji vrši pretragu prema imenu ispitanika²²⁷. Stoga je utvrdio da se društvo Google može smatrati „voditeljem obrade”²²⁸.

Kada voditelj ili izvršitelj obrade ima poslovni nastan izvan EU-a, to društvo mora pisanim putem imenovati predstavnika unutar EU-a²²⁹. U OUZP-u se ističe da predstavnik mora imati poslovni nastan „u jednoj od država članica u kojoj se nalaze ispitanici čiji se osobni podaci obrađuju u vezi s robom ili uslugama koje im se nude ili čije se ponašanje prati”²³⁰. Ako se ne imenuje predstavnik, ipak se može pokrenuti sudski postupak protiv samog voditelja ili izvršitelja obrade²³¹.

222 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 22.

223 *Ibid.*

224 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014.

225 Opća uredba o zaštiti podataka, članak 4. stavak 7.; SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. 21.

226 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. 34.

227 *Ibid.*, t. od 35. do 40.

228 *Ibid.*, t. 41.

229 Opća uredba o zaštiti podataka, članak 27. stavak 1.

230 *Ibid.*, članak 27. stavak 3.

231 *Ibid.*, članak 27. stavak 5.

Zajednički nadzor

OUZP-om se propisuje da se dva ili više voditelja obrade koji zajednički određuju svrhu i načine obrade smatraju zajedničkim voditeljima. To znači da zajedno odlučuju o obradi podataka u zajedničke svrhe²³². U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da je više voditelja obrade ili zajedničko vođenje obrade moguće i u **okviru Vijeća Europe**²³³.

Radna skupina iz članka 29. ističe da zajedničko vođenje obrade može poprimiti različite oblike te da sudjelovanje različitih voditelja obrade u aktivnostima vođenja obrade može biti nejednako²³⁴. Takva fleksibilnost omogućuje sve složeniju obradu podataka²³⁵. Stoga zajednički voditelji obrade moraju u posebnom ugovoru odrediti svoje pojedinačne odgovornosti da bi se postigla sukladnost s obvezama na temelju Uredbe²³⁶.

Zajedničko vođenje obrade dovodi do zajedničke odgovornosti za aktivnost obrade²³⁷. U okviru **prava EU-a** to znači da svaki voditelj obrade ili izvršitelj obrade može biti potpuno odgovoran za cijelu štetu uzrokovanu obradom pod zajedničkim vođenjem obrade kako bi se osiguralo da ispitanik dobije odgovarajuću naknadu²³⁸.

Primjer: Uobičajen primjer zajedničkog vođenja obrade jest baza podataka koju za svoje klijente koji ne ispunjavaju obveze zajednički vodi nekoliko kreditnih institucija. Kada osoba zatraži kredit od banke koja je jedna od zajedničkih voditelja obrade, banke provjeravaju bazu podataka radi lakšeg donošenja odluke na temelju primljenih informacija o kreditnoj sposobnosti podnositelja zahtjeva.

U zakonskim odredbama ne navodi se izričito zahtijeva li zajedničko vođenje obrade da zajednička svrha bude ista za svakog voditelja obrade ili je dovoljno da se njihove

232 *Ibid.*, članak 4. stavak 7. i članak 26.

233 Modernizirana Konvencija br. 108, članak 2. točka (d); Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 22.

234 Radna skupina iz članka 29. (2010.), *Mišljenje 1/2010 o pojmovima „voditelj obrade“ i „izvršitelj obrade“*, WP 169, Bruxelles, 16. veljače 2010., str. 19.

235 *Ibid.*

236 Opća uredba o zaštiti podataka, uvodna izjava 79.

237 *Ibid.*, t. 21.

238 *Ibid.*, članak 82. stavak 4.

svrhe tek djelomično preklapaju. Na europskoj razini zasad nema relevantne sudske prakse. U Mišljenju iz 2010. o voditeljima obrade i izvršiteljima obrade Radna skupina iz članka 29. navodi da zajednički voditelji obrade mogu dijeliti sve svrhe i načine obrade ili mogu dijeliti samo neke svrhe ili načine ili njihove dijelove²³⁹. Dok bi prvo podrazumijevalo vrlo blizak odnos između različitih dionika, drugo bi ukazivalo na manje blizak odnos.

Radna skupina iz članka 29. zagovara šire tumačenje pojma zajedničkog nadzora u cilju fleksibilnosti, kojom bi se odgovorilo na sve složeniju trenutačnu situaciju po pitanju obrade podataka²⁴⁰. Slučaj u koji je bilo uključeno Društvo za svjetsku među-bankovnu financijsku telekomunikaciju (*Society for Worldwide Interbank Financial Telecommunication*, SWIFT) ilustrira stajalište Radne skupine.

Primjer: U takozvanom predmetu SWIFT europske bankovne institucije angažirale su SWIFT, prvobitno kao izvršitelja obrade, za operacije prijenosa podataka tijekom bankovnih transakcija. SWIFT je te podatke o bankovnim transakcijama, pohranjene u računalnom uslužnom centru u Sjedinjenim Američkim Državama (SAD), otkrio Ministarstvu financija SAD-a iako mu to nisu izričito naložile europske bankarske institucije koje su ga angažirale. Prilikom procjene zakonitosti ove situacije, Radna skupina iz članka 29. zaključila je da se europske bankarske institucije koje su angažirale SWIFT, kao i na sam SWIFT, treba gledati kao zajedničke voditelje obrade koji europskim klijentima odgovaraju za otkrivanje njihovih podataka nadležnim tijelima SAD-a²⁴¹.

Izvršitelj obrade

„Izvršitelj obrade” **na temelju prava EU-a** definira se kao osoba koja obrađuje osobne podatke u ime voditelja obrade²⁴². Aktivnosti povjerene izvršitelju obrade mogu se ograničiti na vrlo konkretnu zadaću ili kontekst ili mogu biti prilično općenite i sveobuhvatne.

239 Radna skupina iz članka 29. (2010.), Mišljenje 1/2010 o pojmovima „voditelj obrade” i „izvršitelj obrade”, WP 169, Bruxelles, 16. veljače 2010., str. 19.

240 *Ibid.*

241 Radna skupina iz članka 29. (2006.), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (Mišljenje 10/2006 o obradi osobnih podataka od strane Društva za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT)), WP 128, Bruxelles, 22. studenoga 2006.

242 Opća uredba o zaštiti podataka, članak 4. stavak 8.

Na temelju prava Vijeća Europe značenje pojma izvršitelja obrade isto je kao i prema pravu Unije²⁴³.

Osim što obrađuju podatke za druge, izvršitelji obrade također su i voditelji obrade s obzirom na obradu podataka koju obavljaju u vlastite svrhe, na primjer, upravljanje vlastitim zaposlenicima, plaćama i računima.

Primjer: Društvo Everready specijalizirano je za obradu podataka za vođenje podataka o ljudskim potencijalima za druga društva. U toj je funkciji Everready izvršitelj obrade. Međutim, kada društvo Everready obrađuje podatke svojih zaposlenika, ono je voditelj obrade za postupke obrade podataka jer time ispunjava svoje obveze kao poslodavac.

Odnos između voditelja obrade i izvršitelja obrade

Kao što je rečeno, voditelj obrade definiran je kao onaj koji utvrđuje svrhu i načine obrade. U OUZP-u se jasno navodi da izvršitelj obrade smije obrađivati osobne podatke samo po nalogu voditelja obrade, osim ako je zakonima EU-a ili države članice propisano da to čini izvršitelj obrade²⁴⁴. Ugovor između voditelja obrade i izvršitelja obrade osnovni je element njihova odnosa i predstavlja zakonsku obvezu²⁴⁵.

Primjer: Direktor društva Sunshine odlučio je da društvo Cloudy, specijalizirano za pohranu podataka u oblaku, upravlja podacima o kupcima društva Sunshine. Društvo Sunshine ostaje voditelj obrade, a društvo Cloudy samo je izvršitelj obrade jer, prema ugovoru, Cloudy može upotrebljavati podatke o kupcima društva Sunshine samo u svrhe koje utvrdi Sunshine.

Ako se ovlast utvrđivanja načina obrade povjeri izvršitelju obrade, voditelj obrade svejedno mora primijeniti odgovarajuću razinu nadzora nad odlukama izvršitelja obrade u pogledu načina obrade. Sveukupna odgovornost ostaje na strani voditelja obrade, koji mora nadgledati izvršitelje obrade kako bi osigurao da su njihove odluke u skladu sa zakonodavstvom o zaštiti podataka i njegovim vlastitim nalogima.

²⁴³ Modernizirana Konvencija br. 108, članak 2. točka (f).

²⁴⁴ Opća uredba o zaštiti podataka, članak 29.

²⁴⁵ *Ibid.*, članak 28. stavak 3.

Nadalje, u slučaju da izvršitelj obrade ne poštuje uvjete obrade podataka na način koji propiše voditelj obrade, izvršitelj obrade postao bi voditelj obrade bar u opsegu kršenja uputa voditelja obrade. U tom će slučaju izvršitelj obrade najvjerojatnije postati voditelj obrade koji djeluje nezakonito, a prvobitni voditelj obrade morat će objasniti kako je izvršitelj obrade mogao prekršiti svoj mandat²⁴⁶. Radna skupina iz članka 29. zaista često pretpostavlja da su takvi slučajevi stvar zajedničkog nadzora jer je to u najboljem interesu zaštite ispitanika²⁴⁷.

Pitanje o podjeli odgovornosti može se javiti i kada je voditelj obrade malo poduzeće, a izvršitelj obrade velika korporacija koja može diktirati uvjete usluga koje pruža. U takvim okolnostima Radna skupina iz članka 29. smatra da se standard odgovornosti ne smije snižavati zbog ekonomske nejednakosti i da se mora zadržati shvaćanje pojma voditelja obrade²⁴⁸.

Radi jasnoće i transparentnosti, pojedinosti odnosa voditelja i izvršitelja obrade moraju se urediti pisanim ugovorom²⁴⁹. Ugovor mora posebno uključivati predmet, prirodu, svrhu i trajanje obrade, vrstu osobnih podataka i kategorije ispitanika. U njemu također trebaju biti utvrđene obveze i prava voditelja obrade i izvršitelja obrade, poput zahtjeva u vezi s povjerljivošću i sigurnošću. U suprotnom se krši obveza voditelja obrade u pogledu predočavanja pisane dokumentacije o uzajamnim odgovornostima, što može dovesti do kazni. Kada šteta nastane kao posljedica djelovanja izvan zakonitih naputaka voditelja obrade ili njihova nepridržavanja, odgovornost ne snosi samo voditelj obrade nego i izvršitelj obrade²⁵⁰. Izvršitelj obrade mora voditi evidenciju o svim kategorijama aktivnosti obrade koje provodi u ime voditelja obrade²⁵¹. Ta evidencija mora biti dostupna na zahtjev nadzornog tijela s obzirom na to da i voditelj obrade i izvršitelj obrade moraju surađivati s tim tijelom u obavljanju svojih zadaća²⁵². Voditelji obrade i izvršitelji obrade također

246 *Ibid.*, članak 82. stavak 2.

247 Radna skupina iz članka 29. (2010.), *Mišljenje 1/2010 o pojmovima „voditelj obrade” i „izvršitelj obrade”*, WP 169, Bruxelles, 16. veljače 2010., str. 25.; Radna skupina iz članka 29. (2006.), *Mišljenje 10/2006 o obradi osobnih podataka od strane Društva za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT)*, WP 128, Bruxelles, 22. studenoga 2006.

248 Radna skupina iz članka 29. (2010.), *Mišljenje 1/2010 o pojmovima „voditelj obrade” i „izvršitelj obrade”*, WP 169, Bruxelles, 16. veljače 2010., str. 26.

249 Opća uredba o zaštiti podataka, članak 28. stavak 3. i članak 9.

250 *Ibid.*, članak 82. stavak 2.

251 *Ibid.*, članak 30. stavak 2.

252 *Ibid.*, članak 30. stavak 4. i članak 31.

imaju mogućnost pridržavanja odobrenog kodeksa ponašanja ili mehanizma certifikiranja kako bi dokazali sukladnost sa zahtjevima iz OUPZ-a²⁵³.

Izvršitelji obrade mogu prepustiti određene zadaće podizvršiteljima. To je zakonski dopušteno, pod uvjetom da se utvrde odgovarajuće ugovorne odredbe između voditelja obrade i izvršitelja obrade, uključujući činjenicu je li ovlaštenje voditelja obrade nužno u svakom pojedinom slučaju ili je dovoljna samo obavijest. U OUPZ-u je utvrđeno da početni izvršitelj obrade ostaje u cijelosti odgovoran voditelju obrade ako podizvršitelj obrade ne ispuní svoje obveze zaštite podataka²⁵⁴.

Prema pravu Vijeća Europe, u cijelosti je primjenjivo tumačenje pojmova voditelja obrade i izvršitelja obrade kako je prethodno opisano²⁵⁵.

2.3.2. Primatelji i treće strane

Razlika između ovih dviju kategorija osoba ili subjekata, uvedenih Direktivom o zaštiti podataka, uglavnom se odnosi na odnos koji imaju s voditeljem obrade te time na ovlaštenje za pristup osobnim podacima navedenog voditelja obrade.

„Treća strana” osoba je koja se razlikuje od voditelja obrade i izvršitelja obrade. Prema članku 4. stavku 10. OUPZ-a, treća strana jest „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje nije ispitanik, voditelj obrade, izvršitelj obrade ni osobe koje su ovlaštene za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade”. To znači da će osobe koje rade za organizaciju koja se razlikuje od voditelja obrade – čak i ako pripada istoj grupaciji ili holdingu – biti „treća strana” (ili će joj pripadati). S druge strane, poslovnice banke koje obrađuju račune klijenata pod izravnom ovlašću svojih sjedišta neće se smatrati „trećim stranama”²⁵⁶.

„Primatelj” je širi pojam od „treće strane”. U smislu članka 4. stavka 9. OUPZ-a, primatelj je „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana”. Primatelj može biti ili osoba izvan voditelja obrade ili izvršitelja obrade – u tom je slučaju to treća strana – ili

253 *Ibid.*, članak 28. stavak 5. i članak 42. stavak 4.

254 *Ibid.*, članak 28. stavak 4.

255 Primjerice, vidjeti moderniziranu Konvenciju br. 108, članak 2. točke (b) i (f); Preporuku o izradi profila, članak 1.

256 Radna skupina iz članka 29. (2010.), *Mišljenje 1/2010 o pojmovima „voditelj obrade” i „izvršitelj obrade”*, WP 169, Bruxelles, 16. veljače 2010., str. 31.

netko unutar voditelja obrade ili izvršitelja obrade, kao što je zaposlenik ili drugi odjel unutar istog društva ili tijela.

Razlika između primatelja i trećih strana važna je samo zbog uvjeta za zakonito otkrivanje podataka. Zaposlenici voditelja obrade ili izvršitelja obrade mogu biti primatelji osobnih podataka bez dodatnih pravnih zahtjeva ako su uključeni u postupke obrade voditelja obrade ili izvršitelja obrade. S druge strane, s obzirom na to da je treća strana subjekt zaseban od voditelja obrade ili izvršitelja obrade, ona nije ovlaštena upotrebljavati osobne podatke koje obradi voditelj obrade, osim ako za to u konkretnom slučaju postoji konkretna pravna osnova.

Primjer: Zaposlenik voditelja obrade koji upotrebljava osobne podatke u okviru zadaća koje mu je povjerio poslodavac primatelj je podataka, ali nije treća strana jer upotrebljava podatke u ime i prema uputama voditelja obrade. Primjerice, ako poslodavac otkrije osobne podatke svojih zaposlenika svojem odjelu ljudskih potencijala radi nadolazećih procjena radnog učinka, osoblje ljudskih potencijala bit će primatelj osobnih podataka jer su podaci njima otkriveni tijekom obrade za voditelja obrade.

Međutim, ako organizacija pruži podatke o svojim zaposlenicima društvu za edukaciju koje će upotrijebiti podatke da bi prilagodilo program edukacije zaposlenicima, to je društvo treća strana. To je stoga što društvo koje vodi edukacije nema konkretnu legitimnost ili ovlaštenje (koje u slučaju „ljudskih potencijala” proizlazi iz radnog odnosa s voditeljem obrade) za obradu tih osobnih podataka. Drugim riječima, društvo nije primilo te informacije u sklopu zaposlenja kod voditelja obrade podataka.

2.4. Privola

Ključne točke

- Privola kao pravna osnova za obradu osobnih podataka mora biti dobrovoljno dana, utemeljena na informacijama, posebna i nedvosmislena naznaka želje potvrđena jasnim činom koji predstavlja pristajanje na obradu.
- Za obradu posebnih kategorija podataka potrebna je izričita privola.

Kao što se detaljno razmatra u [poglavlju 4.](#), privola je jedna od šest legitimnih pravnih osnova za obradu osobnih podataka. Privola znači „svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika”²⁵⁷.

Pravom EU-a propisuje se nekoliko elemenata koji su preduvjeti da bi privola bila valjana. Njima se jamči da su ispitanici zaista pristali na određenu uporabu svojih podataka²⁵⁸:

- Privola se mora dati jasnim potvrdnim činom kojim se daje dobrovoljna, posebna, nedvosmislena naznaka, utemeljena na informacijama, da je ispitanik suglasan s obradom svojih podataka. Takav čin može biti radnja ili izjava.
- Ispitanik mora imati pravo na povlačenje privole u svakom trenutku.
- U kontekstu pisane izjave koja obuhvaća i druga pitanja, poput „uvjeta pružanja usluge”, zahtjevi za privolu moraju biti sastavljeni jasno i jednostavno i imati razumljiv i lako dostupan oblik, kojim se privola jasno razlikuje od drugih pitanja. Ako se bilo kojim dijelom te izjave krši OUZP, ona nije obvezujuća.

Privola je važeća u kontekstu zakonodavstva o zaštiti podataka samo ako su ispunjeni svi ovi uvjeti. Odgovornost je voditelja obrade dokazati da je ispitanik pristao na obradu svojih podataka²⁵⁹. Elementi valjane privole dodatno se razmatraju u [dijelu 4.1.1.](#) o zakonitim osnovama obrade osobnih podataka.

Konvencija br. 108 ne sadržava definiciju privole; to je prepušteno nacionalnim zakonodavstvima. Međutim, **sukladno pravu Vijeća Europe**, elementi valjane privole odgovaraju prethodno opisanima²⁶⁰.

Dodatni zahtjevi za valjanu privolu u okviru građanskog prava, kao što je pravna sposobnost, također se primjenjuju u kontekstu zaštite podataka jer su takvi zahtjevi temeljni pravni preduvjeti. Nevaljana privola osoba bez pravne sposobnosti podrazumijeva nedostatak pravne osnove za obradu podataka o takvim osobama. Kad je riječ o pravnoj sposobnosti maloljetnika za sklapanje ugovora, OUZP-om se propisuje

257 Opća uredba o zaštiti podataka, članak 4. stavak 11. Vidjeti i moderniziranu Konvenciju br. 108, članak 5. stavak 2.

258 Opća uredba o zaštiti podataka, članak 7.

259 *Ibid.*, članak 7. stavak 1.

260 Modernizirana Konvencija br. 108, članak 5. stavak 2.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavci od 42. do 45.

da njezine odredbe o najnižoj dobi za dobivanje valjane privole ne utječu na opće ugovorno pravo država članica²⁶¹.

Privola se mora dati jasno, tako da se ne dovode u sumnju namjere ispitanika²⁶². Privola mora biti izričita kada se odnosi na obradu osjetljivih podataka, a može se dati usmeno ili pismeno²⁶³. Pisana se suglasnost može dati elektroničkim putem²⁶⁴. U okviru **prava EU-a i Vijeća Europe** pristanak na obradu nečijih osobnih podataka mora se dati izjavom ili jasnim potvrdnim činom²⁶⁵. Stoga se privola ne može dobiti na temelju tišine, unaprijed označenih potvrdnih okvira, unaprijed ispunjenih obrazaca ili neaktivnosti²⁶⁶.

261 Opća uredba o zaštiti podataka, članak 8. stavak 3.

262 *Ibid.*, članak 6. stavak 1. točka (a) i članak 9. stavak 2. točka (a).

263 *Ibid.*, uvodna izjava 32.

264 *Ibid.*

265 *Ibid.*, članak 4. stavak 11.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

266 Opća uredba o zaštiti podataka, uvodna izjava 32.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

3

Glavna načela europskog zakonodavstva o zaštiti podataka

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a)	Načelo zakonitosti	Modernizirana Konvencija br. 108, članak 5. stavak 3.
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a)	Načelo poštenosti	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (a) ESLJP, <i>K. H. i drugi protiv Slovačke</i> , br. 32881/04, 2009.
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a) SEU, C-201/14, <i>Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.</i> , 2015.	Načelo transparentnosti	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (a) i članak 8. ESLJP, <i>Haralambie protiv Rumunjske</i> , br. 21737/03, 2009.
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (b)	Načelo ograničenja svrhe	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b)
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (c) SEU, spojeni predmeti C-293/12 i C-594/12, <i>Digital Rights Ireland i Kärntner Landesregierung i dr.</i> [VV], 2014.	Načelo smanjenja količine podataka	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (c)
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (d) SEU, C-553/07, <i>College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer</i> , 2009.	Načelo točnosti podataka	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (d)

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (e) SEU, spojeni predmeti C-293/12 i C-594/12, <i>Digital Rights Ireland</i> i <i>Kärntner Landesregierung i dr.</i> [VV], 2014.	Načelo ograničenja pohrane	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (e) ESLJP, <i>S. i Harper protiv Ujedinjene Kraljevine</i> [VV], br. 30562/04 i 30566/04, 2008.
Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (f) i članak 32.	Načelo sigurnosti (cjelovitosti i povjerljivosti) podataka	Modernizirana konvencija br. 108, članak 7.
Opća uredba o zaštiti podataka, članak 5. stavak 2.	Načelo odgovornosti	Modernizirana Konvencija br. 108, članak 10.

U članku 5. Opće uredbe o zaštiti podataka utvrđuju se načela kojima se regulira obrada osobnih podataka. Ta načela obuhvaćaju sljedeće:

- zakonitost, poštenost i transparentnost,
- ograničenje svrhe,
- smanjenje količine podataka,
- točnost podataka,
- ograničavanje pohrane,
- cjelovitost i povjerljivost.

Načela služe kao polazište za detaljnije odredbe u narednim člancima Uredbe. Javljaju se i u člancima 5., 7., 8. i 10. modernizirane Konvencije br. 108. Sve kasnije zakonodavstvo o zaštiti podataka na razini Vijeća Europe ili Europske unije mora biti u skladu s tim načelima, koja se moraju uzeti u obzir pri tumačenju tog zakonodavstva. Prema pravu EU-a, ograničenja načela obrade dopuštena su samo u mjeri u kojoj odgovaraju pravima i obvezama iz članaka od 12. do 22. i moraju biti u skladu sa suštinom temeljnih prava i sloboda. Sva izuzeća i ograničenja u pogledu tih ključnih načela moraju biti propisana na razini EU-a ili nacionalnoj razini²⁶⁷, moraju

²⁶⁷ Modernizirana Konvencija br. 108, članak 11. stavak 1.; Opća uredba o zaštiti podataka, članak 23. stavak 1.

biti zakonom propisana, imati legitimnu svrhu i biti nužne i proporcionalne mjere u demokratskom društvu²⁶⁸. Sva tri uvjeta moraju biti ispunjena.

3.1. Načela zakonitosti, poštenosti i transparentnosti obrade

Ključne točke

- Načela zakonitosti, poštenosti i transparentnosti primjenjuju se na svu obradu osobnih podataka.
- Prema OUZP-u, za zakonitost je potrebno nešto od sljedećeg:
 - privola ispitanika,
 - nužnost sklapanja ugovora,
 - zakonska obveza,
 - nužnost zaštite vitalnih interesa ispitanika ili druge osobe,
 - nužnost izvršavanja zadatka od javnog interesa,
 - nužnost legitimnih interesa voditelja obrade ili treće strane ako nisu nadjačani interesima i pravima ispitanika.
- Obrada osobnih podataka treba se provoditi pošteno.
 - Ispitanika se mora obavijestiti o riziku kako bi se osiguralo da obrada nema nepredviđene neželjene učinke.
- Obrada osobnih podataka treba se provoditi transparentno.
 - Voditelji obrade moraju obavijestiti ispitanike prije obrade njihovih podataka, među ostalim i o svrsi obrade i identitetu i adresi voditelja obrade.
 - Informacije o postupcima obrade moraju se dati jasno i jednostavno kako bi ispitanici lako razumjeli povezana pravila, rizike, zaštitne mjere i prava.
 - Ispitanici imaju pravo pristupa svojim podacima gdje god se oni obrađuju.

²⁶⁸ Opća uredba o zaštiti podataka, članak 23. stavak 1.

3.1.1. Zakonitost obrade podataka

Zakonima o zaštiti podataka EU-a i Vijeća Europe propisano je da se podaci obrađuju zakonito²⁶⁹. Za zakonitu obradu potrebna je privola ispitanika ili druga legitimna osnova utvrđena zakonodavstvom o zaštiti podataka²⁷⁰. U članku 6. stavku 1. OUZP-a navedeno je pet zakonitih osnova obrade osim privole, odnosno: obrada osobnih podataka nužna je za izvršavanje ugovora, za izvršavanje zadaće u ovlasti javnog tijela, za poštovanje pravne obveze, za potrebe legitimnih interesa voditelja obrade ili trećih strana ili za zaštitu ključnih interesa ispitanika ako je potrebno. To je detaljnije objašnjeno u [dijelu 4.1](#).

3.1.2. Poštenost obrade podataka

Uz zakonitu obradu, zakonima o zaštiti podataka EU-a i Vijeća Europe propisano je da se podaci obrađuju na pošten način²⁷¹. Načelom poštene obrade prvenstveno se regulira odnos voditelja obrade i ispitanika.

Voditelji obrade trebali bi obavijestiti ispitanike i javnost o tome da će podatke obrađiti zakonito i transparentno te moraju moći dokazati sukladnost postupaka obrade s OUZP-om. Postupci obrade ne smiju se provoditi u tajnosti i ispitanici trebaju biti svjesni mogućih rizika. Osim toga, voditelji obrade moraju postupati na način koji što više odgovara željama ispitanika, pogotovo ako njegova privola predstavlja pravnu osnovu za obradu podataka.

Primjer: U predmetu *K. H. i drugi protiv Slovačke*²⁷² tužiteljice su bile žene romskog etničkog podrijetla koje su tijekom trudnoće i poroda boravile u dvjema bolnicama u istočnoj Slovačkoj. Nakon toga nijedna od njih nije mogla ponovno začeti dijete unatoč uzastopnim pokušajima. Nacionalni su sudovi bolnicama naložili da tužiteljicama i njihovim zastupnicima dopuste uvid u njihove zdravstvene kartone i prepisivanje dijelova iz njih, no odbacili su njihov zahtjev da dokumente fotokopiraju, navodno radi sprečavanja

269 Modernizirana Konvencija br. 108, članak 5. stavak 3.; Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a).

270 Povelja Europske unije o temeljnim pravima, članak 8. stavak 2.; Opća uredba o zaštiti podataka, uvodna izjava 40. i članci od 6. do 9.; modernizirana Konvencija br. 108, članak 5. stavak 2.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 41.

271 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (a).

272 ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 28. travnja 2009.

zlouporebe. Iz pozitivnih obveza država iz članka 8. EKLJP-a proizlazi da je dužnost da se ispitanicima stave na raspolaganje kopije dosjea s njihovim podacima. Na državi je bilo da odredi načine kopiranja dosjea s osobnim podacima ili, ako je to prikladno, navede uvjerljive razloge za uskraćivanje kopiranja. U slučaju tužiteljica nacionalni su sudovi zabranu kopiranja zdravstvenih kartona prvenstveno opravdali potrebom da se odgovarajuće informacije zaštite od zlouporebe. Međutim, ESLJP nije mogao shvatiti kako bi tužiteljice, koje su ionako dobile pristup cjelokupnoj zdravstvenoj dokumentaciji, mogle zloupotrijebiti informacije o sebi. Osim toga, rizik od takve zlouporebe mogao se spriječiti na drugačiji način umjesto zabranom tužiteljicama da kopiraju dosjee, na primjer ograničenjem opsega osoba koje imaju pravo pristupa dosjeima. Država nije uspjela predočiti dovoljno uvjerljive razloge zbog kojih je tužiteljicama zabranjen učinkovit pristup informacijama o njihovu zdravlju. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Što se tiče internetskih usluga, svojstva sustava za obradu podataka moraju omogućiti ispitanicima da uistinu razumiju što se događa s njihovim podacima. U svakom slučaju, načelo poštenosti nadilazi obvezu transparentnosti i može se također povezati s etičnom obradom osobnih podataka.

Primjer: Istraživački odjel sveučilišta provodi eksperiment u kojem analizira promjene raspoloženja 50 ispitanika. Ispitanici moraju zabilježiti svoja razmišljanja u elektroničku datoteku svaki sat u određeno vrijeme. Tih je 50 osoba dalo privolu za taj konkretni projekt i tu konkretnu upotrebu podataka u sklopu sveučilišta. Istraživački odsjek uskoro otkriva da bi elektroničko bilježenje razmišljanja bilo vrlo korisno za drugi projekt usmjeren na mentalno zdravlje pod vodstvom drugog tima. Iako je sveučilište kao voditelj obrade moglo upotrijebiti iste podatke za rad drugog tima bez dodatnih koraka za osiguravanje zakonitosti obrade tih podataka s obzirom na to da su svrhe usklađene, sveučilište je obavijestilo ispitanike i zatražilo novu privolu sukladno svojem etičkom kodeksu u istraživanjima i načelu poštene obrade.

3.1.3. Transparentnost obrade podataka

Zakonima o zaštiti podataka EU-a i Vijeća Europe zahtijeva se da osobni podaci budu „transparentno obrađivani s obzirom na ispitanika”²⁷³.

Tim se načelom utvrđuje obveza voditelja obrade da poduzme sve odgovarajuće mjere kako bi ispitanici, koji mogu biti korisnici, kupci ili klijenti, bili obaviješteni o načinu upotrebe njihovih podataka²⁷⁴. Transparentnost se može odnositi na informacije pružene pojedincu prije početka obrade²⁷⁵, informacije koje trebaju biti dostupne ispitanicima tijekom obrade²⁷⁶ te informacije dane ispitanicima nakon njihova zahtjeva za pristup vlastitim podacima²⁷⁷.

Primjer: U predmetu *Haralambie protiv Rumunjske*²⁷⁸ tužitelju je dopušten pristup informacijama koje je organizacija tajne službe čuvala u vezi s njime tek pet godina nakon njegova zahtjeva. ESLJP je ponovio da je od vitalne važnosti da pojedinci o kojima javna tijela čuvaju osobne dosjee mogu pristupiti takvim dosjeima. Tijela su bila dužna osigurati učinkovit postupak dobivanja pristupa takvim informacijama. ESLJP je smatrao da ni količina prenesenih dosjea ni nedostaci sustava arhiviranja nisu opravdavali petogodišnje kašnjenje odobravanja tužiteljeva zahtjeva za pristup dosjeima. Tijela tužitelju nisu osigurala učinkovit i pristupačan postupak kojim bi mu se omogućio pristup osobnim dosjeima u razumnom roku. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Postupci obrade moraju se ispitanicima objasniti na jednostavan i pristupačan način kako bi im se omogućilo da razumiju što će se dogoditi s njihovim podacima. To znači da konkretna svrha obrade osobnih podataka mora biti poznata ispitaniku u trenutku prikupljanja osobnih podataka²⁷⁹. Transparentnost obrade podataka zahtijeva

273 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (a) i članak 8.

274 Opća uredba o zaštiti podataka, članak 12.

275 *Ibid.*, članci 13. i 14.

276 Radna skupina iz članka 29., *Opinion 2/2017 on data processing at work* (Mišljenje 2/2017 o obradi podataka na radnom mjestu), WP 249, str. 23.

277 Opća uredba o zaštiti podataka, članak 15.

278 ESLJP, *Haralambie protiv Rumunjske*, br. 21737/03, 27. listopada 2009.

279 Opća uredba o zaštiti podataka, uvodna izjava 39.

jasno i jednostavno izražavanje²⁸⁰. Dotičnim osobama moraju biti jasna pravila, rizici, zaštitne mjere i prava u vezi s obradom njihovih osobnih podataka²⁸¹.

U pravu Vijeća Europe također je utvrđeno da voditelj obrade mora određene ključne informacije obavezno pružiti ispitanicima na proaktivan način. Informacije o imenu i adresi voditelja obrade (ili više zajedničkih voditelja obrade), pravnoj osnovi i svrhama obrade podataka, kategorijama podataka koji se obrađuju i primateljima te o načinima ostvarivanja prava mogu se pružiti u bilo kojem primjerenom obliku (putem internetske stranice, tehnoloških alata na osobnim uređajima itd.), pod uvjetom da su informacije pošteno i učinkovito predstavljene ispitaniku. Te informacije moraju biti lako dostupne, čitljive, razumljive i prilagođene pojedinim ispitanicima (primjerice, na jeziku prilagođenom djeci kada je to potrebno). Potrebno je pružiti i sve dodatne informacije koje su potrebne da bi se osigurala poštena obrada podataka ili koje su korisne za takvu svrhu, poput razdoblja čuvanja, saznanja o razlozima za obradu podataka ili informacija o prijenosima podataka primatelju koji pripada drugoj stranki ili nije stranka (među ostalim, pruža li osoba koja nije stranka odgovarajuću razinu zaštite ili mjere koje poduzima voditelj obrade kako bi se zajamčila takva odgovarajuća razina zaštite podataka)²⁸².

Sukladno pravu na pristup²⁸³, ispitanik ima pravo da, na zahtjev, od voditelja obrade sazna obrađuju li se njegovi podaci te ako da, koji se podaci obrađuju²⁸⁴. Usto, sukladno pravu na informiranje²⁸⁵, voditelji obrade ili izvršitelji obrade moraju proaktivno obavijestiti osobe čiji se podaci obrađuju, među ostalim, o svrhama, trajanju i načinima obrade, u načelu prije početka postupka obrade.

Primjer: Predmet *Smaranda Bara i dr. protiv Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*²⁸⁶ odnosio se na prijenos poreznih podataka u vezi s prihodom od samostalnih djelatnosti Državne agencije za porezno upravljanje rumunjskom Državnom zavodu za socijalnu sigurnost, na temelju kojih je zatražena uplata zaostalih

280 *Ibid.*

281 *Ibid.*

282 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 68.

283 Opća uredba o zaštiti podataka, članak 15.

284 Modernizirana Konvencija br. 108, članak 8. i članak 9. stavak 1. točka (b).

285 Opća uredba o zaštiti podataka, članci 13. i 14.

286 SEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. listopada 2015., t. od 28. do 46.

doprinosa u sustav osiguranja. Od SEU-a se tražilo da utvrdi je li ispitanik trebao dobiti informacije o identitetu voditelja obrade podataka i svrsi prijenosa podataka prije nego što je Državni zavod za socijalnu sigurnost obradio te podatke. SEU je zaključio da kada tijelo javne uprave neke države članice prenosi osobne podatke drugom tijelu javne uprave koje dalje obrađuje te podatke, ispitanike se mora obavijestiti o tom prijenosu ili obradi.

U određenim situacijama dopuštena su odstupanja od obveze informiranja ispitanika o obradi podataka. Odstupanja se dodatno obrađuju u [dijelu 6.1.](#) o pravima ispitanika.

3.2. Načelo ograničenja svrhe

Ključne točke

- Svrha obrade podataka mora se jasno definirati prije početka obrade.
- Nije dopuštena daljnja obrada podataka na način koji nije u skladu s izvornom svrhom, iako su u Općoj uredbi o zaštiti podataka predviđena izuzeća od tog pravila za svrhe arhiviranja u javnom interesu, za znanstvena ili povijesna istraživanja i statističke analize.
- U suštini, načelo ograničenja svrhe znači da se svaka obrada osobnih podataka mora obavljati u određenu, jasno definiranu svrhu te samo u dodatne utvrđene svrhe koje su usklađene s izvornom.

Načelo ograničenja svrhe jedno je od temeljnih načela europskog zakonodavstva o zaštiti podataka. Uvelike je povezano s transparentnošću, predvidljivošću i korisničkim nadzorom: ako je svrha obrade dovoljno specifična i jasna, pojedinci znaju što mogu očekivati i povećavaju se transparentnost i pravna sigurnost. Istovremeno, jasno razgraničenje svrhe važno je kako bi se ispitanicima omogućilo učinkovito ostvarivanje njihovih prava, poput prava na prigovor na obradu²⁸⁷.

Ovim načelom određuje se da se svaka obrada osobnih podataka mora obavljati u određenu, jasno definiranu svrhu te samo u dodatne svrhe koje su usklađene s izvornom²⁸⁸. Obrada osobnih podataka u nedefinirane i/ili neograničene svrhe stoga nije zakonita. Obrada osobnih podataka bez određene svrhe, samo na temelju

287 Radna skupina iz članka 29. (2013.), *Opinion 3/2013 on purpose limitation* (Mišljenje 3/2013 o ograničavanju svrhe), WP 203, 2. travnja 2013.

288 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (b).

mišljenja da bi mogli biti korisni u budućnosti, također nije zakonita. Legitimnost obrade osobnih podataka ovisit će o svrsi obrade, koja mora biti izričita, utvrđena i legitimna.

Svaka nova svrha obrade podataka koja nije usklađena s izvornom mora imati vlastitu zasebnu pravnu osnovu i ne može se oslanjati na činjenicu da su podaci prvotno stečeni ili obrađeni u drugu legitimnu svrhu. Zakonita je obrada pak ograničena na svoju prvotno određenu svrhu pa svaka nova svrha obrade iziskuje novu zasebnu pravnu osnovu. Primjerice, otkrivanje podataka trećim stranama u novu svrhu mora se pažljivo razmotriti jer takvo otkrivanje često iziskuje dodatnu pravnu osnovu različitou od one za prikupljanje podataka.

Primjer: Zrakoplovna kompanija prikuplja podatke od svojih putnika radi bilježenja rezervacija i pravilnog upravljanja letom. Zrakoplovna kompanija treba podatke o brojevima sjedala putnika, posebnim tjelesnim ograničenjima, kao što su potrebe osoba u invalidskim kolicima, te o posebnim prehrambenim zahtjevima, kao što su košer ili halal hrana. Ako se od zrakoplovne kompanije zatraži prijenos tih podataka, koji se nalaze u evidenciji imena putnika, tijelima nadležnima za imigraciju u odredišnoj zračnoj luci, ti se podaci zatim upotrebljavaju u svrhu kontrole imigracije, koja se razlikuje od početne svrhe prikupljanja podataka. Stoga je za prijenos tih podataka tijelu nadležnom za imigraciju potrebna nova i zasebna pravna osnova.

Pri razmatranju područja primjene i ograničenja određene svrhe, modernizirana Konvencija br. 108 i Opća uredba o zaštiti podataka temelje se na načelu usklađenosti: upotreba podataka u usklađene svrhe dopuštena je na temelju prvotne pravne osnove. Stoga se daljnja obrada podataka ne može vršiti na način koji je neočekivan ili neprimjeren za ispitanika ili kojemu se on može protiviti²⁸⁹. Da bi se ocijenilo može li se daljnja obrada smatrati usklađenom, voditelj obrade treba uzeti u obzir sljedeće (među ostalim):

- „svaku vezu između te svrhe i svrhe planiranog nastavka obrade,
- kontekst u kojem su prikupljeni osobni podaci, posebno opravdana očekivanja ispitanika koja se temelje na njihovu odnosu s voditeljem obrade u pogledu daljnje uporabe podataka,

289 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 49.

- prirodu osobnih podataka,
- posljedice planiranog nastavka obrade za ispitanike, i
- postojanje primjerenih zaštitnih mjera u izvornoj i planiranoj daljnjoj obradi²⁹⁰. To se primjerice može postići šifriranjem ili pseudonimizacijom.

Primjer: Društvo Sunshine steklo je podatke o kupcima tijekom upravljanja odnosima s kupcima (CRM). Zatim te podatke prenosi društvu Moonlight, koje se bavi izravnim marketingom, a koje te podatke želi iskoristiti kao pomoć u marketinškim kampanjama trećih društava. Prijenos podataka koji vrši društvo Sunshine radi marketinga drugih društava predstavlja naknadnu upotrebu podataka u novu svrhu, koja nije usklađena s CRM-om, prvotnom svrhom prikupljanja podataka o kupcima društva Sunshine. Stoga prijenos podataka društvu Moonlight iziskuje vlastitu pravnu osnovu.

Za razliku od toga, upotreba podataka iz CRM-a u svrhe vlastitog marketinga društva Sunshine, odnosno slanje marketinških poruka vlastitim kupcima za vlastite proizvode, općenito je prihvaćena kao usklađena svrha.

U Općoj uredbi o zaštiti podataka i moderniziranoj Konvenciji br. 108 utvrđuje se da se „daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe” *a priori* smatra usklađenom s prvotnom svrhom²⁹¹. Međutim, prilikom daljnje obrade osobnih podataka moraju se uspostaviti odgovarajuće zaštitne mjere poput anonimizacije, šifriranja ili pseudonimizacije podataka te ograničenja pristupa podacima²⁹². U Općoj uredbi o zaštiti podataka dodaje se sljedeće: „Ako je ispitanik dao privolu ili se obrada temelji na pravu Unije ili pravu države članice koje čini potrebnu i razmjernu mjeru u demokratskom društvu posebno za zaštitu važnih ciljeva od općeg javnog interesa, voditelju obrade trebalo bi dopustiti daljnju obradu osobnih podataka neovisno o usklađenosti svrha”²⁹³.

290 Opća uredba o zaštiti podataka, uvodna izjava 50. i članak 6. stavak 4.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 49.

291 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (b); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b). Primjer nacionalnih odredbi jest austrijski *Zakon o zaštiti podataka (Datenschutzgesetz)*, Savezni službeni list I br. 165/1999, st. 46.

292 Opća uredba o zaštiti podataka, članak 6. stavak 4.; modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b); Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 50.

293 Opća uredba o zaštiti podataka, uvodna izjava 50.

Prilikom daljnje obrade ispitanik stoga treba biti obaviješten o svrhama te svojim pravima, poput prava na prigovor²⁹⁴.

Primjer: Društvo Sunshine prikupilo je i pohranilo podatke o svojim kupcima u okviru upravljanja odnosima s kupcima (CRM). Društvo Sunshine smije dalje upotrebljavati te podatke radi statističke analize ponašanja svojih kupaca prilikom kupovine jer je statistika usklađena svrha. Nije potrebna dodatna pravna osnova, kao što je privola ispitanika. Međutim, za daljnju obradu osobnih podataka u statističke svrhe društvo Sunshine mora uspostaviti odgovarajuće zaštitne mjere za prava i slobode ispitanika. Tehničke i organizacijske mjere koje društvo Sunshine mora provesti mogu uključivati pseudonimizaciju.

3.3. Načelo smanjenja količine podataka

Ključne točke

- Obrada podataka mora biti ograničena na ono što je nužno za ispunjavanje legitimne svrhe.
- Obrada osobnih podataka treba se obavljati samo kada se svrha obrade ne može razumno postići drugim sredstvima.
- Obradom podataka ne smije se neproporcionalno miješati u interese, prava i slobode o kojima je riječ.

Obraduju se samo podaci koji su „primjereni, relevantni i ne preopsežni u odnosu na svrhu njihova prikupljanja i/ili daljnje obrade”²⁹⁵. Kategorije podataka odabranih za obradu moraju biti nužne za postizanje navedenog općeg cilja postupka obrade, a voditelj obrade treba strogo ograničiti prikupljanje podataka na one informacije koje su izravno relevantne za konkretnu svrhu obrade.

²⁹⁴ *Ibid.*

²⁹⁵ Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (c); Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (c).

Primjer: U predmetu *Digital Rights Ireland*²⁹⁶ SEU je razmatrao valjanost Direktive o zadržavanju podataka kojom se nastojalo uskladiti nacionalne odredbe o zadržavanju osobnih podataka koji se generiraju ili obrađuju javno dostupnim elektroničkim komunikacijskim uslugama ili mrežama radi njihova mogućeg prijenosa nadležnim tijelima za borbu protiv teških zločina poput organiziranog kriminala i terorizma. Ne uzimajući u obzir činjenicu da se to smatralo svrhom kojom se doista ostvaruje cilj od općeg interesa, uopćeni način na koji je Direktiva obuhvaćala „svaku osobu i sva sredstva elektroničke komunikacije kao i sve podatke o prometu bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na cilj borbe protiv teških kaznenih djela” smatrao se problematičnim²⁹⁷.

Nadalje, upotrebom posebne tehnologije za povećanje privatnosti ponekad je moguće posve izbjeći upotrebu osobnih podataka ili upotrijebiti mjere za smanjenje mogućnosti pripisivanja podataka ispitaniku (primjerice, pseudonimizacijom), čime se postiže povoljno rješenje za privatnost. To je naročito prikladno u opsežnijim sustavima obrade.

Primjer: Gradsko vijeće redovnim korisnicima sustava javnog gradskog prijevoza nudi čip-karticu uz određenu naknadu. Na površini kartice navedeno je ime korisnika u pisanom obliku, a u čipu u elektroničkom obliku. Pri svakom korištenju autobusom ili tramvajem čip-kartica postavlja se ispred ugrađenih uređaja za očitavanje, na primjer, u autobusima i tramvajima. Podaci koje uređaj očitava elektronički se provjeravaju u bazi podataka s imenima ljudi koji su kupili putnu kartu.

Taj sustav nije usklađen s načelom smanjenja količine podataka na optimalan način: provjera smije li osoba upotrebljavati sredstva javnog prijevoza mogla bi se izvršiti bez usporedbe osobnih podataka s čip-kartice s onima iz baze podataka. Bilo bi dovoljno, na primjer, imati posebnu elektroničku sliku, kao što je bar-kod, u čipu kartice kojim bi se, kad se kartica postavi ispred uređaja za čitanje, potvrdila valjanost kartice. Takvim se sustavom ne bi bilježilo tko je i kada upotrebljavao određeno prijevozno sredstvo. To bi bilo optimalno rješenje u smislu načela smanjenja količine podataka jer iz tog načela proizlazi obveza smanjenja prikupljanja podataka.

²⁹⁶ SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014.

²⁹⁷ *Ibid.*, t. 44. i 57.

Članak 5. stavak 1. modernizirane Konvencije br. 108 sadržava zahtjev proporcionalnosti za obradu osobnih podataka u vezi s legitimnom svrhom koja se nastoji postići. Mora se uspostaviti poštena ravnoteža među svim predmetnim interesima u svim fazama obrade. To znači da se „[o]sobni podaci koji su dostatni i relevantni, ali koji bi uključivali neproporcionalno miješanje u predmetna temeljna prava i slobode trebaju smatrati preopsežnima”²⁹⁸.

3.4. Načelo točnosti podataka

Ključne točke

- Načelo točnosti podataka mora provoditi voditelj obrade u svim postupcima obrade.
- Netočni podaci moraju se izbrisati ili ispraviti bez odgode.
- Podaci će se možda morati redovito provjeravati i ažurirati radi osiguravanja točnosti.

Voditelj obrade koji raspolaže osobnim podacima ne smije te podatke upotrebljavati bez poduzimanja mjera kojima se može relativno jasno osigurati da su podaci točni i ažurni²⁹⁹.

Obvezu osiguravanja točnosti podataka treba promatrati u kontekstu svrhe obrade podataka.

Primjer: U predmetu *Rijkeboer*³⁰⁰ SEU je razmatrao zahtjev državljanina Nizozemske za primanjem informacija od lokalnih gradskih vlasti u Amsterdamu o identitetu osoba kojima su lokalne vlasti pružale zapise o njemu tijekom prethodne dvije godine te o sadržaju otkrivenih podataka. SEU je ustvrdio da „pravo na privatnost znači da ispitanik može biti siguran da se njegovi osobni podaci obrađuju na pravilan i zakonit način, odnosno da su osnovni podaci o njemu točni i da se otkrivaju ovlaštenim primateljima”. SEU je zatim

298 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, članak 52.; Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (c).

299 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (d); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (d).

300 SEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 7. svibnja 2009.

uputio na preambulu Direktive o zaštiti podataka, u kojoj se navodi da ispitanici moraju uživati pravo pristupa svojim osobnim podacima kako bi mogli provjeriti njihovu točnost³⁰¹.

Također mogu postojati slučajevi u kojima je ažuriranje pohranjenih podataka zakonom zabranjeno jer je osnovna svrha pohrane podataka dokumentiranje događaja kao povijesnog zapisa.

Primjer: Medicinska dokumentacija o operaciji ne smije se izmijeniti, odnosno „ažurirati“, čak i ako se nalazi spomenuti u njoj kasnije pokažu pogrešnim. U takvim okolnostima u dokumentaciju se smiju dodati samo napomene koje moraju biti jasno označene kao naknadno dodani unosi.

S druge strane, postoje situacije u kojima su redovna provjera točnosti podataka i njihovo ažuriranje apsolutno nužni zbog moguće štete koju može pretrpjeti ispitanik ako podaci ostanu netočni.

Primjer: Ako osoba želi sklopiti ugovor o kreditu s bankovnom institucijom, banka obično provjerava kreditnu sposobnost potencijalnog klijenta. Za to postoje posebne baze podataka u kojima su sadržani podaci o kreditnoj povijesti privatnih osoba. Ako su u takvoj bazi podataka navedeni netočni ili zastarjeli podaci o osobi, ona može pretrpjeti negativne posljedice. Voditelji obrade takvih baza podataka stoga se moraju posebno potruditi poštovati načelo točnosti.

301 Nekadašnja uvodna izjava 41., preambula Direktive 95/46/EZ.

3.5. Načelo ograničenja pohrane

Ključne točke

- Načelo ograničenja pohrane znači da se osobni podaci moraju izbrisati ili anonimizirati čim prestanu biti potrebni za svrhe za koje su prikupljeni.

Člankom 5. stavkom 1. točkom (e) OUZP-a i člankom 5. stavkom 4. točkom (e) modernizirane Konvencije br. 108 propisuje se da osobni podaci moraju biti „čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju“. Dakle, podaci se moraju izbrisati ili anonimizirati nakon ispunjavanja tih svrha. U tu svrhu „voditelj obrade trebao bi odrediti rok za brisanje ili periodično preispitivanje“ kako bi se osiguralo da se podaci ne čuvaju dulje no što je nužno³⁰².

U predmetu *S. i Marper* ESLJP je zaključio da ključna načela odgovarajućih instrumenata Vijeća Europe, kao i pravo i praksa drugih ugovornih stranki, nalažu da zadržavanje podataka bude proporcionalno u odnosu na svrhu prikupljanja i vremenski ograničeno, naročito u policijskom sektoru³⁰³.

Primjer: U predmetu *S. i Marper*³⁰⁴ ESLJP je presudio da zadržavanje otisaka prstiju, staničnih uzoraka i profila DNK-a dvojice tužitelja na neodređeno razdoblje nije razmjerno ni nužno u demokratskom društvu s obzirom na to da je kazneni postupak protiv obojice tužitelja prekinut oslobođenjem odnosno obustavom postupka.

Vremensko ograničenje za pohranu osobnih podataka odnosi se samo na podatke koji se čuvaju u obliku koji omogućuje identifikaciju ispitanika. Stoga bi se zakonita pohrana podataka koji više nisu potrebni mogla postići anonimizacijom podataka.

Arhiviranje podataka zbog javnog interesa, u znanstvene ili povijesne svrhe ili za upotrebu u statističkim analizama, može se vršiti na dulja razdoblja, pod uvjetom da

³⁰² Opća uredba o zaštiti podataka, uvodna izjava 39.

³⁰³ ESLJP, *S. i Marper protiv Ujedinjene Kraljevine* [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.; primjerice, vidjeti i: ESLJP, *M. M. protiv Ujedinjene Kraljevine*, br. 24029/07, 13. studenoga 2012.

³⁰⁴ ESLJP, *S. i Marper protiv Ujedinjene Kraljevine* [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.

će se takvi podaci upotrebljavati isključivo u navedene svrhe³⁰⁵. Za trajnu pohranu i upotrebu osobnih podataka nužno je provesti odgovarajuće tehničke i organizacijske mjere kako bi se zaštitila prava i slobode ispitanika.

Moderniziranom Konvencijom br. 108 dopuštaju se i iznimke od načela ograničenja pohrane pod uvjetom da su one propisane zakonom, da se njima poštuje suština temeljnih prava i sloboda te da su one nužne i proporcionalne za ostvarenje ograničenog broja legitimnih ciljeva³⁰⁶. Oni, među ostalim, uključuju zaštitu nacionalne sigurnosti, istragu i progon kaznenih djela, izvršavanje kaznenih sankcija, zaštitu ispitanika te zaštitu prava i temeljnih sloboda drugih.

Primjer: U predmetu *Digital Rights Ireland*³⁰⁷ SEU je preispitao valjanost Direktive o zadržavanju podataka kojom se nastojalo uskladiti nacionalne odredbe o zadržavanju osobnih podataka koji se generiraju ili obrađuju javno dostupnim elektroničkim komunikacijskim uslugama ili mrežama radi borbe protiv teških zločina poput organiziranog kriminala i terorizma. Direktivom o zadržavanju podataka propisano je razdoblje zadržavanja podataka „koje nije kraće od šest mjeseci, a da se pritom ne navodi nikakvo razlikovanje između kategorija podataka predviđenih u članku 5. te direktive s obzirom na njihovu eventualnu korist za cilj koji se slijedi ili s obzirom na osobe na koje se odnosi”³⁰⁸. SEU je također iznio problem izostanka objektivnih kriterija u Direktivi o zadržavanju podataka na temelju kojih se određuje točno razdoblje zadržavanja podataka – koje može varirati od najmanje šest mjeseci do najviše 24 mjeseca – kako bi se osiguralo da je razdoblje ograničeno na ono što je strogo nužno³⁰⁹.

305 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (e); modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b) i članak 11. stavak 2.

306 Modernizirana Konvencija br. 108, članak 11.1.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavci od 91. do 98.

307 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014.

308 *Ibid.*, t. 63.

309 *Ibid.*, t. 64.

3.6. Načelo sigurnosti podataka

Ključne točke

- Sigurnost i povjerljivost osobnih podataka ključne su za sprečavanje štetnih posljedica za ispitanika.
- Sigurnosne mjere mogu biti tehničke i/ili organizacijske naravi.
- Pseudonimizacija je postupak kojim se mogu zaštititi osobni podaci.
- Primjerenost sigurnosnih mjera mora se odrediti za svaki pojedini slučaj i redovito preispitivati.

Prema načelu sigurnosti podataka, potrebno je provesti odgovarajuće tehničke ili organizacijske mjere prilikom obrade osobnih podataka kako bi se podaci zaštitili od nehotičnog, neovlaštenog ili nezakonitog pristupa, upotrebe, izmjene, otkrivanja, gubitka, uništenja ili oštećenja³¹⁰. U OUZP-u se navodi da voditelj obrade i izvršitelj obrade prilikom provedbe takvih mjera trebaju uzeti u obzir „najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca”³¹¹. Ovisno o okolnostima pojedinog slučaja, odgovarajuće tehničke i organizacijske mjere mogu uključivati, primjerice, pseudonimizaciju i enkripciju osobnih podataka i/ili redovno testiranje i procjenjivanje učinkovitosti mjera za osiguravanje sigurnosti obrade podataka³¹².

Kao što je objašnjeno u [dijelu 2.1.1.](#), pseudonimizacija podataka znači zamjenu informacija osobnih podataka – koji omogućuju identifikaciju ispitanika – pseudonimom i čuvanje tih informacija na odvojenom mjestu, tako da su zaštićeni tehničkim ili organizacijskim mjerama. Postupak pseudonimizacije ne smije se zamijeniti postupkom anonimizacije, u kojem se uklanjanju sve poveznice s identitetom osobe.

310 Opća uredba o zaštiti podataka, uvodna izjava 39. i članak 5. stavak 1. točka (f); modernizirana Konvencija br. 108, članak 7.

311 Opća uredba o zaštiti podataka, članak 32. stavak 1.

312 *Ibid.*

Primjer: Rečenica „Charles Spencer, rođen 3. travnja 1967., otac je četvero djece, dvaju dječaka i dviju djevojčica” može se, primjerice, pseudonimizirati na sljedeći način:

„C. S. 1967. otac je četvero djece, dvaju dječaka i dviju djevojčica”, ili

„324 otac je četvero djece, dvaju dječaka i dviju djevojčica”, ili

„YESz3201 otac je četvero djece, dvaju dječaka i dviju djevojčica”.

Korisnici koji pristupe pseudonimiziranim podacima obično neće moći identificirati „Charlesa Spencera, rođenog 3. travnja 1967.” na temelju pseudonima „324” ili „YESz3201”. Stoga su takvi podaci češće zaštićeni od zlouporabe.

Međutim, prvi je navedeni primjer manje siguran. Ako se rečenica „C. S. 1967. otac je četvero djece, dvaju dječaka i dviju djevojčica” rabi u malenom selu u kojem Charles Spencer živi, moglo bi ga se lako prepoznati. Metoda pseudonimizacije može utjecati na učinkovitost zaštite podataka.

Osobni podaci sa šifriranim ili zasebno čuvanim informacijama upotrebljavaju se u mnogim kontekstima radi očuvanja tajnosti osobnog identiteta. To je osobito korisno kada voditelji obrade moraju osigurati da se bave istim ispitanicima, tj. osobama čiji se podaci obrađuju, no ne zahtijevaju – ili ne bi smjeli saznati – stvarni identitet tih osoba. To se događa kada, na primjer, istraživač istražuje tijek bolesti pacijenata čiji je identitet poznat samo bolnici u kojoj se pacijenti liječe i koja istraživaču dostavlja pseudonimizirane povijesti slučajeva. Pseudonimizacija je dakle snažna karika u lancu tehnologije za zaštitu privatnosti. Ona može biti važan element u provedbi tehničke zaštite privatnosti. To znači da je zaštita podataka ugrađena u tkivo sustava obrade podataka.

U članku 25. OUZP-a, u kojem se obrađuje tehnička zaštita podataka, izričito se navodi pseudonimizacija kao primjer odgovarajuće tehničke i organizacijske mjere koju voditelji obrade trebaju provesti radi omogućivanja primjene načela zaštite podataka i uključenja potrebnih zaštitnih mjera. Time će voditelji obrade ispuniti zahtjeve iz Uredbe i zaštititi prava ispitanika prilikom obrade njihovih osobnih podataka.

Poštovanje odobrenog kodeksa ponašanja ili odobrenog mehanizma certificiranja može se iskoristiti za dokazivanje sukladnosti sa zahtjevom sigurnosti obrade³¹³. U svojem Mišljenju o implikacijama obrade evidencije imena putnika za zaštitu podataka Vijeće Europe navodi druge primjere odgovarajućih sigurnosnih mjera za zaštitu osobnih podataka u sustavima evidencije imena putnika. One uključuju čuvanje podataka u sigurnom fizičkom okruženju, ograničenje pristupa putem različitih razina prijave i zaštitu prijenosa podataka snažnom kriptografijom³¹⁴.

Primjer: Internetske stranice društvenih mreža i pružatelji usluga elektroničke pošte omogućuju korisnicima postavljanje dodatne razine sigurnosti podataka u uslugama koje pružaju zahvaljujući uvođenju dvostruke provjere autentičnosti. Uz unos osobne lozinke, korisnici moraju obaviti drugu prijavu da bi pristupili svojem korisničkom računu. To može uključivati, primjerice, unos sigurnosnog koda koji se šalje na broj mobilnog telefona povezan s korisničkim računom. Na taj način provjera u dva koraka osigurava bolju zaštitu osobnih podataka od neovlaštenog pristupa hakera korisničkim računima.

U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 pružaju se dodatni primjeri odgovarajućih zaštitnih mjera, kao što je primjena obveze čuvanja poslovne tajne ili usvajanje primjerenih tehničkih sigurnosnih mjera kao što je šifriranje podataka³¹⁵. Prilikom uspostavljanja pojedinih sigurnosnih mjera, voditelj obrade ili, kada je to primjenjivo, izvršitelj obrade treba uzeti u obzir nekoliko elemenata, kao što su priroda i količina osobnih podataka koji se obrađuju, moguće štetne posljedice za ispitanike i potreba za ograničenim pristupom podacima³¹⁶. Prilikom provedbe odgovarajućih sigurnosnih mjera moraju se razmotriti najsuvremenije postojeće metode i tehnike sigurnosti podataka u području obrade podataka. Trošak takvih mjera mora biti proporcionalan ozbiljnosti i vjerojatnosti mogućih rizika. Neophodno je redovito preispitivanje sigurnosnih mjera kako bi se po potrebi mogle ažurirati³¹⁷.

U slučajevima povrede osobnih podataka i moderniziranom Konvencijom br. 108 i OUZP-om zahtijeva se da voditelj obrade bez nepotrebne odgode obavijesti

313 *Ibid.*, članak 32. stavak 3.

314 Vijeće Europe, Odbor za Konvenciju br. 108, *Opinion on the Data protection implications of the processing of Passenger Name Records* (Mišljenje o implikacijama obrade evidencija imena putnika za zaštitu podataka), T-PD(2016)18rev, 19. kolovoza 2016., str. 9.

315 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 56.

316 *Ibid.*, stavak 62.

317 *Ibid.*, stavak 63.

nadležno nadzorno tijelo o povredi te o rizicima za prava i slobode pojedinaca³¹⁸. Slična obveza obavješćivanja ispitanika primjenjuje se i kada je vjerojatno da će povreda osobnih podataka prouzročiti visok rizik za njegova prava i slobode³¹⁹. Ispitanike se o takvim povredama mora obavijestiti uporabom jasnog i jednostavnog jezika³²⁰. Ako izvršitelj obrade sazna za povredu osobnih podataka, odmah mora obavijestiti voditelja obrade³²¹. U određenim situacijama mogu se primjenjivati iznimke od obveze obavješćivanja. Primjerice, voditelj obrade ne mora obavijestiti nadzorno tijelo „ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca”³²². Isto tako, nije potrebno obavijestiti ispitanika kada primijenjene sigurnosne mjere učine podatke nerazumljivima neovlaštenim osobama ili kada zbog naknadnih mjera više nije vjerojatno da će doći do visokog rizika³²³. Ako bi obavješćivanje ispitanika o povredi osobnih podataka iziskivalo nerazmjeran napor voditelja obrade, javnim obavješćivanjem ili sličnom mjerom može se osigurati da se „ispitanici obavješćuju na jednako djelotvoran način”³²⁴.

3.7. Načelo odgovornosti

Ključne točke

- Prema načelu odgovornosti, voditelji obrade i izvršitelji obrade moraju tijekom svojih aktivnosti obrade aktivno i neprekidno provoditi mjere za promicanje i osiguravanje zaštite podataka.
- Voditelji obrade i izvršitelji obrade odgovorni su za usklađenost svojih postupaka obrade sa zakonima o zaštiti podataka i svojim pojedinačnim obvezama.
- Voditelji obrade moraju moći u svakom trenutku dokazati sukladnost s odredbama o zaštiti podataka ispitanicima, javnosti i nadzornim tijelima. Izvršitelji obrade također se moraju pridržavati određenih obveza koje su strogo povezane s odgovornošću (poput vođenja evidencije o postupcima obrade i imenovanja službenika za zaštitu podataka).

318 Modernizirana Konvencija br. 108, članak 7. stavak 2.; Opća uredba o zaštiti podataka, članak 33. stavak 1.

319 Modernizirana Konvencija br. 108, članak 7. stavak 2.; Opća uredba o zaštiti podataka, članak 34. stavak 1.

320 Opća uredba o zaštiti podataka, članak 34. stavak 2.

321 *Ibid.*, članak 33. stavak 1.

322 *Ibid.*

323 *Ibid.*, članak 34. stavak 3. točke (a) i (b).

324 *Ibid.*, članak 34. stavak 3. točka (c).

U OUZP-u i moderniziranoj Konvenciji br. 108 utvrđeno je da je voditelj obrade odgovoran za usklađenost s načelima obrade osobnih podataka opisanima u ovom poglavlju te da to mora biti u mogućnosti dokazati³²⁵. U tu svrhu voditelj obrade mora provesti odgovarajuće tehničke i organizacijske mjere³²⁶. Iako se načelo odgovornosti iz članka 5. stavka 2. OUZP-a odnosi samo na voditelje obrade, odgovornost se očekuje i od izvršitelja obrade s obzirom na to da se oni moraju pridržavati nekoliko obveza te da su usko povezani s odgovornošću.

Zakonima EU-a i Vijeća Europe također se propisuje da je voditelj obrade odgovoran za usklađenost s načelima zaštite podataka opisanima u [dijelovima od 3.1. do 3.6.](#) te da bi trebao biti u mogućnosti to osigurati³²⁷. Radna skupina iz članka 29. ističe da bi se „vrsta postupaka i mehanizama razlikovala prema rizicima koje predstavljaju obrada i priroda podataka”³²⁸.

Voditelji obrade mogu olakšati usklađenost s ovim zahtjevom na različite načine, uključujući sljedeće:

- vođenje evidencije aktivnosti obrade i njezino davanje na uvid nadzornom tijelu na zahtjev³²⁹,
- u određenim situacijama imenovanje službenika za zaštitu podataka koji će biti uključen u sva pitanja u pogledu zaštite osobnih podataka³³⁰,
- provođenje procjene učinka zaštite podataka za one vrste obrade za koje je vjerojatno da će prouzročiti visok rizik za prava i slobode pojedinaca³³¹,
- osiguravanje tehničke i integrirane zaštite podataka³³²,
- provedbu modaliteta i postupaka za ostvarivanje prava ispitanika³³³,

325 *Ibid.*, članak 5. stavak 2.; modernizirana Konvencija br. 108, članak 10. stavak 1.

326 Opća uredba o zaštiti podataka, članak 24.

327 *Ibid.*, članak 5. stavak 2.; modernizirana Konvencija br. 108, članak 10. stavak 1.

328 Radna skupina iz članka 29., *Opinion 3/2010 on the principle of accountability* (Mišljenje 3/2010 o načelu odgovornosti), WP 173, Bruxelles, 13. srpnja 2010., st. 12.

329 Opća uredba o zaštiti podataka, članak 30.

330 *Ibid.*, članci od 37. do 39.

331 *Ibid.*, članak 35.; modernizirana Konvencija br. 108, članak 10. stavak 2.

332 Opća uredba o zaštiti podataka, članak 25.; modernizirana Konvencija br. 108, članak 10. stavci 2. i 3.

333 *Ibid.*, članak 12. i članak 24.

- pridržavanje odobrenih kodeksa ponašanja ili mehanizama certificiranja³³⁴.

Iako se načelo odgovornosti iz članka 5. stavka 2. OUZP-a ne odnosi izričito na izvršitelje obrade, određene odredbe povezane s odgovornošću također sadržavaju obveze za njih, poput vođenja evidencije o aktivnostima obrade i imenovanja službenika za zaštitu podataka za sve aktivnosti obrade za koje je on potreban³³⁵. Izvršitelji obrade također moraju osigurati da su provedene sve mjere potrebne za sigurnost podataka³³⁶. U pravno obvezujućem ugovoru između voditelja i izvršitelja obrade mora se utvrditi da izvršitelj obrade pomaže voditelju obrade u vezi s određenim zahtjevima sukladnosti, primjerice prilikom obavljanja procjene učinka zaštite podataka ili obavješćivanja voditelja obrade o svakoj povredi osobnih podataka čim za nju sazna³³⁷.

Godine 2013. Organizacija za gospodarsku suradnju i razvoj (OECD) donijela je smjernice o privatnosti kojima se naglašava da voditelji obrade imaju važnu ulogu u osiguravanju funkcioniranja zaštite podataka u praksi. U smjernicama se načelo odgovornosti opisuje na sljedeći način: „voditelj obrade treba biti odgovoran za sukladnost s mjerama kojima se provode spomenuta [materijalna] načela”³³⁸.

Primjer: Primjer iz zakonodavstva kojim se naglašava načelo odgovornosti jest izmjena i dopuna³³⁹ Direktive o privatnosti i elektroničkim komunikacijama 2002/58/EZ iz 2009. Prema članku 4. u njegovu izmijenjenom obliku, Direktivom se nameće obveza da mjere „osiguravaju provedbu sigurnosne politike s obzirom na obradu osobnih podataka”. Dakle, u pogledu odredbi o sigurnosti iz te direktive, zakonodavac je odlučio da je potrebno izričito uvjetovati postojanje i provedbu sigurnosne politike.

334 *Ibid.*, članak 40. i članak 42.

335 *Ibid.*, članak 5. stavak 2., članci 30. i 37.

336 *Ibid.*, članak 28. stavak 3. točka (c).

337 *Ibid.*, članak 28. stavak 3. točka (d).

338 OECD (2013.), *Smjernice kojima se uređuju zaštita privatnosti i prekogranični prijenosi osobnih podataka*, članak 14.

339 Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge, Direktive 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredbe (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača, SL 2009 L 337, str. 11.

Prema mišljenju Radne skupine iz članka 29.³⁴⁰, suština je odgovornosti obveza voditelja obrade da:

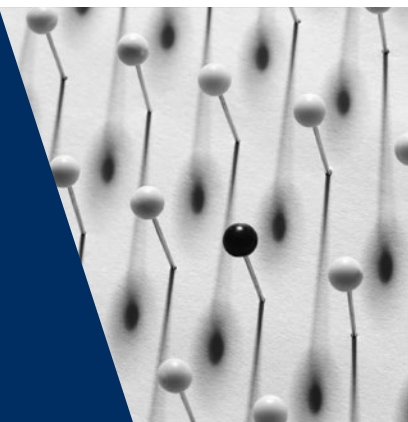
- uvede mjere kojima bi se u uobičajenim okolnostima jamčilo poštovanje pravila o zaštiti podataka u kontekstu postupaka obrade, te
- ima spremnu dokumentaciju kojom se ispitanicima i nadzornim tijelima može dokazati koje su potrebne mjere poduzete kako bi se osigurala usklađenost s propisima o zaštiti podataka.

Prema načelu odgovornosti, od voditelja obrade stoga se zahtijeva sposobnost aktivnog dokazivanja usklađenosti umjesto čekanja da ispitanici ili nadzorna tijela ukažu na nedostatke.

³⁴⁰ Radna skupina iz članka 29., *Mišljenje 3/2010 o načelu odgovornosti*, WP 173, Bruxelles, 13. srpnja 2010.

4

Odredbe europskog zakonodavstva o zaštiti podataka



EU	Obuhvaćena pitanja	Vijeće Europe
Propisi o zakonitoj obradi podataka		
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (a) SEU, C-543/09, <i>Deutsche Telekom AG protiv Bundesrepublik Deutschland</i> , 2011. SEU, C-536/15, <i>Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)</i> , 2017.	Privola	Profiling Recommendation (Preporuka o izradi profila), članak 3.4. točka (b) i članak 3.6. Modernizirana Konvencija br. 108, članak 5. stavak 2.
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (b)	(Pred)ugovorni odnos	Preporuka o izradi profila, članak 3.4. točka (b)
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (c)	Pravne dužnosti voditelja obrade	Preporuka o izradi profila, članak 3.4. točka (a)
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (d)	Vitalni interesi ispitanika	Preporuka o izradi profila, članak 3.4. točka (b)
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (e) SEU, C-524/06, <i>Huber protiv Bundesrepublik Deutschland [VV]</i> , 2008.	Javni interes i izvršavanje javne ovlasti	Preporuka o izradi profila, članak 3.4. točka (b)

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (f) SEU, C-13/16, <i>Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIA „Rīgas satiksme”</i> , 2017. SEU, spojeni predmeti C-468/10 i C-469/10, <i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado</i> , 2011.	Legitimni interesi drugih	Preporuka o izradi profila, članak 3.4. točka (b) ESLJP, <i>Y protiv Turske</i> , br. 648/10, 2015.
Opća uredba o zaštiti podataka, članak 6. stavak 4.	Izuzeće od ograničenja svrhe: daljnja obrada u druge svrhe	Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b)
Propisi o zakonitoj obradi osjetljivih podataka		
Opća uredba o zaštiti podataka, članak 9. stavak 1.	Opća zabrana obrade	Modernizirana Konvencija br. 108, članak 6.
Opća uredba o zaštiti podataka, članak 9. stavak 2.	Izuzeća od opće zabrane	Modernizirana Konvencija br. 108, članak 6.
Propisi o sigurnoj obradi		
Opća uredba o zaštiti podataka, članak 32.	Obveza osiguravanja sigurne obrade	Modernizirana Konvencija br. 108, članak 7. stavak 1. ESLJP, <i>I. protiv Finske</i> , br. 20511/03, 2008.
Opća uredba o zaštiti podataka, članak 28. i članak 32. stavak 1. točka (b)	Obveza povjerljivosti	Modernizirana Konvencija br. 108, članak 7. stavak 1.
Opća uredba o zaštiti podataka, članak 34. Direktiva o privatnosti i elektroničkim komunikacijama, članak 4. stavak 2.	Obavješćivanje u slučaju povrede podataka	Modernizirana Konvencija br. 108, članak 7. stavak 2.
Propisi o odgovornosti i promicanju usklađenosti		
Opća uredba o zaštiti podataka, članci 12., 13. i 14.	Transparentnost općenito	Modernizirana Konvencija br. 108, članak 8.
Opća uredba o zaštiti podataka, članci 37., 38. i 39.	Službenici za zaštitu podataka	Modernizirana Konvencija br. 108, članak 10. stavak 1.
Opća uredba o zaštiti podataka, članak 30.	Evidencija aktivnosti obrade	

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka, članci 35. i 36.	Procjena učinka i prethodno savjetovanje	Modernizirana Konvencija br. 108, članak 10. stavak 2.
Opća uredba o zaštiti podataka, članci 33. i 34.	Obavješćivanje u slučaju povrede podataka	Modernizirana Konvencija br. 108, članak 7. stavak 2.
Opća uredba o zaštiti podataka, članci 40. i 41.	Kodeksi ponašanja	
Opća uredba o zaštiti podataka, članci 42. i 43.	Certificiranje	
Tehnička i integrirana zaštita podataka		
Opća uredba o zaštiti podataka, članak 25. stavak 1.	Tehnička zaštita podataka	Modernizirana Konvencija br. 108, članak 10. stavak 2.
Opća uredba o zaštiti podataka, članak 25. stavak 2.	Integrirana zaštita podataka	Modernizirana Konvencija br. 108, članak 10. stavak 3.

Načela su nužno općenite prirode. Kad se primjenjuju na konkretne situacije, postoji određena sloboda tumačenja i izbor sredstava. **Prema pravu Vijeća Europe**, stranaka modernizirane Konvencije br. 108 prepušta se da pojasne tu slobodu tumačenja u svojim nacionalnim zakonodavstvima. U **pravu Europske unije** situacija je drugačija: za uspostavu zaštite podataka na unutarnjem tržištu smatralo se da su nužna detaljnija pravila na razini EU-a radi usklađivanja razine zaštite podataka u okviru nacionalnih zakonodavstava država članica. Općom uredbom o zaštiti podataka uspostavlja se sloj detaljnih pravila prema načelima utvrđenima u njezinu članku 5., koja su izravno primjenjiva unutar nacionalnog pravnog poretka. Stoga se sljedeće napomene o detaljnim pravilima zaštite podataka na europskoj razini pretežito odnose na pravo EU-a.

4.1. Propisi o zakonitoj obradi

Ključne točke

- Osobni se podaci mogu zakonito obraditi ako ispunjavaju neki od sljedećih kriterija:
 - obrada se temelji na privoli ispitanika,
 - obrada osobnih podataka uvjetuje se ugovornim odnosom,
 - obrada je nužna za ispunjavanje zakonskih obveza voditelja obrade,
 - obrada podataka nužna je zbog vitalnih interesa ispitanika ili druge osobe,
 - obrada je potrebna za obavljanje zadaće od javnog interesa,
 - razlog za obradu legitimni su interesi voditelja obrade ili trećih osoba, no samo ako ih ne nadjačavaju interesi ili temeljna prava ispitanika.
- Zakonita obrada osjetljivih osobnih podataka podliježe posebnom, strožem režimu.

4.1.1. Zakonska osnova obrade podataka

U poglavlju II. Opće uredbe o zaštiti podataka, pod naslovom „Načela”, utvrđuje se da svaka obrada osobnih podataka prvenstveno mora biti u skladu s načelima kvalitete podataka iz članka 5. Uredbe. Prema jednome od načela, osobni podaci trebaju biti „zakonito, pošteno i transparentno obrađivani”. Zatim, da bi se podaci obradili na zakonit način, obrada mora biti u skladu s jednom od zakonskih osnova na temelju kojih obrada podataka postaje zakonita, a koje su navedene u članku 6.³⁴¹ za neosjetljive osobne podatke odnosno u članku 9. za posebne kategorije podataka (ili osjetljive podatke). Slično tome, u poglavlju II. modernizirane Konvencije br. 108, u kojemu se utvrđuju „osnovna načela zaštite osobnih podataka”, propisuje se da obrada podataka mora biti „proporcionalna s obzirom na legitimnu svrhu koja se nastoji ostvariti” da bi bila zakonita.

341 SEU, spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr.* i *Christa Neukomm i Joseph Lauerermann protiv Österreichischer Rundfunk*, 20. svibnja 2003., t. 65.; SEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008., t. 48.; SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECMD) protiv Administración del Estado*, 24. studenoga 2011., t. 26.

Neovisno o zakonskoj osnovi obrade na koju se voditelj obrade oslanja pri pokretanju postupka obrade osobnih podataka, voditelj obrade također treba primijeniti zaštitne mjere utvrđene u općem sustavu zakonodavstva o zaštiti podataka.

Privola

U okviru prava Vijeća Europe privola se spominje u članku 5. stavku 2. modernizirane Konvencije br. 108. Također se navodi u sudskoj praksi ESLJP-a i u nekoliko preporuka Vijeća Europe³⁴². **U okviru prava EU-a** privola kao osnova za zakonitu obradu podataka jasno je utvrđena člankom 6. OUZP-a i također se izričito spominje u članku 8. Povelje. Svojstva valjane privole objašnjena su u definiciji privole iz članka 4., uvjeti za dobivanje valjane privole detaljno su opisani u članku 7., a posebna pravila o privoli djeteta u vezi s uslugama informacijskog društva utvrđena su člankom 8. OUZP-a.

Kao što je objašnjeno u [dijelu 2.4.](#), privola mora biti dana dobrovoljno, utemeljena na informacijama, posebna i nedvosmislena. Privola mora biti izjava ili jasan potvrdni čin kojim se pristaje na obradu podataka, a pojedinac je ima pravo povući u bilo kojem trenutku. Voditelji obrade imaju dužnost vođenja evidencije o privoli koja se može provjeriti.

Dobrovoljna privola

U pravnom okviru **Vijeća Europe**, tj. modernizirane Konvencije br. 108, privola ispitanika mora „predstavljati slobodan izraz svjesne odluke”³⁴³. Postojanje dobrovoljne privole valjano je samo „ako ispitanik može zaista birati bez opasnosti od obmane, zastrašivanja, prisile ili ozbiljnih negativnih posljedica ako uskrati privolu”³⁴⁴. U tom pogledu **pravom EU-a** utvrđeno je da se privola ne smatra dobrovoljno danom „ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica”³⁴⁵. U OUZP-u se naglašava da „[k]ada se procjenjuje je li privola bila dobrovoljna, u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, izvršenje ugovora, uključujući pružanje usluge, uvjetovano privolom za obradu osobnih

342 Vidjeti, primjerice, Vijeće Europe, Odbor ministara (2010.), Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila, 23. studenoga 2010., članak 3.4. točka (b).

343 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

344 Vidjeti i *Mišljenje 15/2011 o pojmu privole*, Radne skupine iz članka 29. (2011.), WP 187, Bruxelles, 13. srpnja 2011., str. 12.

345 Opća uredba o zaštiti podataka, uvodna izjava 42.

podataka koja nije nužna za izvršenje tog ugovora”³⁴⁶. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da se „[n]ikakav nedopušteni utjecaj ili pritisak (koji može biti ekonomske ili druge naravi), bilo izravan ili neizravan, ne smije izvršiti na ispitanika, a privola se ne može smatrati dobrovoljno danom ako ispitanik nema istinski izbor ili nije u mogućnosti uskratiti ili povući privolu bez štetnih posljedica”³⁴⁷.

Primjer: Određene općine u državi A odlučile su uvesti boravišne iskaznice s ugrađenim čipom. Stanovnici općine nisu obvezni ishoditi te elektroničke iskaznice. Međutim, stanovnicima koji ne posjeduju iskaznicu uskraćen je pristup nizu važnih administrativnih usluga, poput mogućnosti plaćanja lokalnih poreza putem interneta, podnošenja pritužbi elektroničkim putem (čime se ostvaruje prednost trodnevnog roka u kojemu nadležno tijelo mora odgovoriti te zaobilaženje čekanja u redovima), kupovine ulaznica za gradsku koncertnu dvoranu po nižim cijenama i upotrebe uređaja za skeniranje na ulazu.

Obrada osobnih podataka za potrebe općine u ovom primjeru ne može biti utemeljena na privoli. Budući da se na stanovnike vrši barem neizravan pritisak da nabave elektroničku iskaznicu i pristanu na obradu podataka, njihova privola nije dobrovoljna. Razvoj sustava elektroničkih iskaznica unutar općine stoga se treba temeljiti na drugoj zakonskoj osnovi kojom se opravdava obrada. Primjerice, općina se može pozvati na činjenicu da je obrada podataka nužna za izvršavanje zadaće od javnog interesa, što je zakonita osnova za obradu sukladno članku 6. stavku 1. točki (e) OUZP-a³⁴⁸.

Dobrovoljna privola također može biti dovedena u pitanje u situacijama podređenosti, tj. kada postoji značajna ekonomska ili druga neravnoteža između voditelja obrade, koji osigurava privolu, i ispitanika, koji daje privolu³⁴⁹. Tipičan primjer takve

³⁴⁶ *Ibid.*, članak 7. stavak 4.

³⁴⁷ Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

³⁴⁸ Radna skupina iz članka 29. (2011.), *Mišljenje 15/2011 o pojmu privole*, WP 187, Bruxelles, 13. srpnja 2011., str. 16. Dodatni primjeri slučajeva u kojima se obrada podataka ne može temeljiti na privoli, nego zahtijeva drugu zakonsku osnovu kojom se opravdava obrada, dostupni su na 14. i 17. str. Mišljenja.

³⁴⁹ Vidjeti i *Mišljenje 8/2001 o obradi osobnih podataka u kontekstu zaposlenja*, Radne skupine iz članka 29. (2001.), WP 48, Bruxelles, 13. rujna 2001.; Radna skupina iz članka 29. (2005.), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 114, Bruxelles, 25. studenoga 2005.; Radna skupina iz članka 29. (2017.), *Mišljenje 2/2017 o obradi podataka na radnom mjestu*, WP 249, Bruxelles, 8. lipnja 2017.

neravnoteže i podređenosti jest poslodavčeva obrada osobnih podataka u kontekstu radnog odnosa. Prema mišljenju Radne skupine iz članka 29., „[z]aposlenici gotovo nikada nisu u poziciji da dobrovoljno daju, uskrate ili opozovu privolu s obzirom na ovisnost koja proizlazi iz odnosa poslodavca i zaposlenika. S obzirom na neravnotežu moći, zaposlenici mogu dati dobrovoljnu privolu samo u iznimnim okolnostima, kada nema nikakvih posljedica uslijed prihvaćanja ili odbijanja neke ponude”³⁵⁰.

Primjer: Velika kompanija planira izraditi imenik s imenima svih zaposlenika, njihovim funkcijama u kompaniji i poslovnim adresama, i to isključivo u svrhe unapređenja unutarnje komunikacije kompanije. Voditelj kadrovske službe predlaže da se u imenik uz svako ime zaposlenika doda i fotografija kako bi se suradnici lakše međusobno prepoznali na sastancima. Predstavnici zaposlenika traže da se to učini isključivo ako na to pristane svaki zaposlenik posebno.

U takvoj se situaciji privola zaposlenika treba priznati kao pravna osnova za obradu fotografija u imeniku jer objava fotografije u imeniku sama po sebi vjerojatno ne nosi nikakve posljedice za zaposlenika, neovisno o tome pristane li na objavu fotografije u imeniku ili ne.

Primjer: Društvo A planira sastanak troje svojih zaposlenika i direktora tvrtke B radi razgovora o mogućoj budućoj suradnji na projektu. Sastanak će se održati u poslovnim prostorima društva B, koje od društva A traži da mu e-poštom dostavi imena, životopise i fotografije sudionika sastanka. Društvo B tvrdi da su mu imena i fotografije sudionika potrebni kako bi zaštitarsko osoblje na ulazu u zgradu moglo provjeriti radi li se o pravim osobama, a životopisi će direktorima omogućiti da se bolje pripreme za sastanak. U ovom slučaju prijenos osobnih podataka zaposlenika društva A ne može se temeljiti na privoli. Privola se ne može smatrati dobrovoljnom jer je moguće da se zaposlenici suoče s negativnim posljedicama ako odbiju tu ponudu (primjerice, mogu se zamijeniti drugim zaposlenicima ne samo na sastanku nego i u tijeku daljnje suradnje s društvom B i općenito u sklopu projekta). Stoga se obrada mora temeljiti na drugoj zakonitoj osnovi.

350 Radna skupina iz članka 29., *Mišljenje 2/2017 o obradi podataka na radnom mjestu*, WP 249, Bruxelles, 8. lipnja 2017.

No to ne znači da privola nikada ne može biti valjana u okolnostima u kojima bi uskrata privole imala određene negativne posljedice. Primjerice, ako uskraćivanje privole za preuzimanje kartice nekog supermarketa za posljedicu ima samo neostvarivanje malog popusta na cijene određenih artikala, privola ipak može biti valjana pravna osnova za obradu osobnih podataka onih kupaca koji su pristali na preuzimanje kartice. Između društva i kupca nema podređenosti, a posljedice uskrate privole nisu dovoljno ozbiljne da bi spriječile slobodan izbor ispitanika (pod uvjetom da je popust na cijene dovoljno nizak da ne utječe na njegov slobodan izbor).

Međutim, kada se proizvodi ili usluge mogu dobiti isključivo ako se određeni osobni podaci otkriju voditelju obrade ili dalje trećim osobama, privola ispitanika na otkrivanje vlastitih podataka koji nisu nužni za taj ugovor ne može se smatrati slobodnom odlukom, te stoga nije valjana sukladno zakonodavstvu o zaštiti podataka³⁵¹. OUZP-om se strogo zabranjuje uvjetovanje pružanja proizvoda i usluga davanjem privole³⁵².

Primjer: Ako putnici zračne kompanije pristanu da ona prenese takozvane evidencije imena putnika (odnosno podatke o njihovoj identitetu, prehrambenim navikama ili zdravstvenim problemima) nadležnim tijelima za imigraciju određene strane zemlje, to se ne može smatrati valjanom privolom sukladno zakonodavstvu o zaštiti podataka jer putnici nemaju izbora ako žele posjetiti tu zemlju. Da bi se takvi podaci zakonito prenijeli, potrebna je druga pravna osnova osim privole, a to je najvjerojatnije poseban zakon.

Privola utemeljena na informacijama

Ispitanik mora imati dovoljno informacija prije iskorištavanja mogućnosti odabira. Obično će privola utemeljena na informacijama uključivati precizan i vrlo razumljiv opis pitanja za koje se privola traži. Kako objašnjava Radna skupina iz članka 29., privola se mora temeljiti na uvažavanju i razumijevanju činjenica i implikacija radnje ispitanika kojom on pristaje na obradu. Stoga, „[d]otični pojedinac mora na jasan i razumljiv način dobiti točne i potpune informacije o svim relevantnim pitanjima [...] kao što su priroda podataka koji se obrađuju, svrhe obrade, primatelji podataka

351 Opća uredba o zaštiti podataka, članak 7. stavak 4.

352 *Ibid.*

i prava ispitanika”³⁵³. Da bi privola bila utemeljena na informacijama, pojedinci također moraju biti svjesni posljedica uskraćivanja privole za obradu.

S obzirom na važnost privole utemeljene na informacijama, OUZP-om i Izvješćem s objašnjenjima o moderniziranoj Konvenciji br. 108 nastojalo se pojasniti taj pojam. U uvodnim izjavama OUZP-a utvrđuje se da privola utemeljena na informacijama podrazumijeva da bi ispitanik „trebao [...] barem znati identitet voditelja obrade i svrhe obrade za koju se upotrebljavaju osobni podaci”³⁵⁴.

U iznimnom slučaju u kojem se privola upotrebljava kao odstupanje kako bi se osigurala zakonita osnova za međunarodni prijenos podataka, da bi privola bila valjana, voditelj obrade mora obavijestiti ispitanika o mogućim rizicima takva prijenosa zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera³⁵⁵.

U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 utvrđuje se da se moraju pružiti informacije o implikacijama odluke ispitanika, prvenstveno stoga „što činjenica davanja suglasnosti podrazumijeva i mjeru u kojoj se suglasnost daje”³⁵⁶.

Važna je i kvaliteta informacija. Kvaliteta informacija znači da se jezik informacija treba prilagoditi predviđenim primateljima. Informacije se moraju pružiti bez žargona, na jasnom i jednostavnom jeziku koji prosječni korisnik može razumjeti³⁵⁷. Informacije također moraju biti lako dostupne ispitaniku, a mogu se pružiti usmeno ili pisano. Dostupnost i vidljivost informacija važni su elementi: informacije moraju biti jasno vidljive i istaknute. U elektroničkom okruženju dobro rješenje mogu biti slojevite informativne obavijesti jer one ispitanicima omogućuju odabir pristupa sažetoj ili proširenoj verziji informacija.

Posebna privola

Da bi bila valjana, privola također mora biti posebno namijenjena svrsi obrade, koja mora biti jasno i nedvosmisleno opisana. To ide ruku pod ruku s kvalitetom pruženih

353 Radna skupina iz članka 29. (2007.), *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (Radni dokument o obradi osobnih podataka koji se odnose na zdravlje u elektroničkim zdravstvenim kartonima), WP 131, Bruxelles, 15. veljače 2007.

354 Opća uredba o zaštiti podataka, uvodna izjava 42.

355 *Ibid.*, članak 49. stavak 1. točka (a).

356 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

357 Radna skupina iz članka 29. (2011.), *Mišljenje 15/2011 o pojmu privole*, WP 187, Bruxelles, 13. srpnja 2011., str. 19.

informacija o svrsi privole. U tom su kontekstu relevantna razumna očekivanja prosječnog ispitanika. Ako treba dodavati ili mijenjati postupke obrade na način koji se nije mogao opravdano predvidjeti u trenutku davanja prve privole te je time došlo do promjene svrhe, od ispitanika se ponovno mora tražiti privola. Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih³⁵⁸.

Primjeri: U predmetu *Deutsche Telekom AG*³⁵⁹ SEU je razmatrao je li pružatelj telekomunikacijskih usluga koji je morao proslijediti osobne podatke pretplatnika radi objave u registrima trebao zatražiti novu privolu ispitanika³⁶⁰ s obzirom na to da primatelji podataka u trenutku davanja privole nisu bili navedeni.

SEU je smatrao da sukladno članku 12. Direktive o privatnosti i elektroničkim komunikacijama nova privola nije potrebna prije prosljeđivanja podataka. Budući da su ispitanici imali samo mogućnost dati privolu za svrhu obrade, odnosno objavu njihovih podataka, nisu mogli odabrati registar u kojemu bi se ti podaci mogli objaviti.

SEU je istaknuo kako „iz kontekstualnog i sustavnog tumačenja članka 12. Direktive o privatnosti i elektroničkim komunikacijama proizlazi da se suglasnost iz članka 12. stavka 2. odnosi na svrhu objave osobnih podataka u javnom imeniku, a ne na identitet konkretnog pružatelja usluge imenika”³⁶¹. Nadalje, „sama se objava osobnih podataka u javnom imeniku u posebne svrhe može pokazati štetnom za pretplatnika”³⁶², a ne identitet autora objave.

Predmet *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV protiv Autoriteit Consument en Markt (ACM)*³⁶³ odnosio se na zahtjev belgijskog društva da im društva koja pružaju usluge davanja obavijesti o brojevima pretplatnika te telefonskih imenika za poduzeća koja dodjeljuju telefonske brojeve

358 Opća uredba o zaštiti podataka, uvodna izjava 32.

359 SEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. svibnja 2011. Vidjeti posebno t. 53. i 54.

360 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija, SL 2002 L 201 (Direktiva o privatnosti i elektroničkim komunikacijama).

361 SEU, C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. svibnja 2011., t. 61.

362 *Ibid.*, t. 62.

363 SEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. ožujka 2017.

u Nizozemskoj pruže pristup podacima vezanim za njihove pretplatnike. Belgijsko se društvo oslonilo na obvezu utvrđenu Direktivom o univerzalnoj usluzi³⁶⁴. Prema njoj, društva koja dodjeljuju telefonske brojeve obvezna su brojeve učiniti dostupnima telefonskim imenicima koji ih zatraže ako pretplatnici daju privolu za objavu svojih brojeva. Nizozemska društva to su odbila tvrdeći da ne moraju pružiti predmetne podatke poduzeću koje ima poslovni nastan u drugoj državi članici. Tvrđila su da su korisnici dali privolu za objavu svojih brojeva smatrajući da će se oni objaviti u nizozemskom telefonskom imeniku. SEU je zaključio da se Direktivom o univerzalnoj usluzi obuhvaćaju svi zahtjevi poduzeća koja pružaju usluge davanja obavijesti o brojevima pretplatnika, neovisno o državi članici u kojoj imaju poslovni nastan. Također je zaključio da se prosljeđivanjem tih podataka drugom poduzeću s namjerom objave javnog telefonskog imenika bez ishođenja nove privole pretplatnika ne može značajno narušiti pravo na zaštitu osobnih podataka³⁶⁵. Stoga nije nužno da poduzeće koje dodjeljuje telefonske brojeve pretplatnicima u svojem zahtjevu za privolu pretplatnika posebno navodi državu članicu u koju se podaci o njemu mogu poslati³⁶⁶.

Nedvosmislena privola

Svaka se privola mora dati nedvosmisleno³⁶⁷. To znači da ne smije izazivati opravdanu sumnju da je ispitanik želio izraziti svoje slaganje s obradom svojih podataka. Primjerice, neaktivnost ispitanika ne podrazumijeva nedvosmisleni privolu.

To bi bio slučaj kada voditelj obrade ishodi privolu izjavama u svojim pravilima zaštite privatnosti poput: „Upotrebom naše usluge pristajete na obradu svojih osobnih podataka.” U takvu će slučaju voditelji obrade možda morati osigurati da korisnici ručno i pojedinačno pristanu na takva pravila.

Ako se privola daje u okviru obrasca koji je dio ugovora, privola za obradu osobnih podataka mora biti individualizirana, a u svakom slučaju, „zaštitnim mjerama [...]

364 Direktiva 2002/22/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama (Direktiva o univerzalnoj usluzi), SL 2002 L 108, str. 51., kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. (Direktiva o univerzalnim uslugama), SL 2009 L 337, str. 11.

365 SEU, C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. ožujka 2017., t. 36.

366 *Ibid.*, t. 40. i 41.

367 Opća uredba o zaštiti podataka, članak 4. stavak 11.

trebalo bi se osigurati da je ispitanik svjestan činjenice da daje privolu i do koje mjere se ona daje³⁶⁸.

Zahtjevi privole za djecu

OUZP-om se u kontekstu pružanja usluga informacijskog društva propisuje posebna zaštita djece jer ona „mogu biti manje svjesna rizika, posljedica i predmetnih zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka”³⁶⁹. Sukladno **pravu EU-a**, kada pružatelji usluga informacijskog društva obrađuju osobne podatke djece mlađe od 16 godina na temelju privole, takva je obrada zakonita „samo ako i u mjeri u kojoj je privolu dao ili odobrio nositelj roditeljske odgovornosti nad djetetom”³⁷⁰. Države članice mogu propisati nižu dob u nacionalnom zakonodavstvu, ali ne nižu od 13 godina³⁷¹. Privola nositelja roditeljske odgovornosti nije nužna „u kontekstu preventivnih usluga ili usluga savjetovanja koje su ponuđene izravno djetetu”³⁷². Informacije i komunikacija, u slučaju da je obrada usmjerena prema djetetu, trebale bi biti na jasnom i jednostavnom jeziku koji dijete lako može razumjeti³⁷³.

Pravo na povlačenje privole u svakom trenutku

OUZP sadržava opće pravo na povlačenje privole u svakom trenutku³⁷⁴. Ispitanik mora biti obaviješten o takvu pravu prije davanja privole i on može iskoristiti to pravo prema vlastitom nahođenju. Ne bi se trebali postavljati zahtjevi za obrazloženje povlačenja niti bi smjelo biti rizika od negativnih posljedica, osim ukidanja svih povlastica koje su proizlazile iz prethodno dogovorene upotrebe podataka. Povlačenje privole treba biti jednako jednostavno kao njezino davanje³⁷⁵. Dobrovoljna privola nije moguća ako ispitanik ne može povući svoju privolu bez štetnih posljedica ili ako povlačenje nije jednako jednostavno kao davanje privole³⁷⁶.

368 *Ibid.*, uvodna izjava 42.

369 *Ibid.*, uvodna izjava 38.

370 *Ibid.* Članak 8. stavak 1. prva alineja. Pojam usluga informacijskog društva definiran je u članku 4. stavku 25. Opće uredbe o zaštiti podataka.

371 Opća uredba o zaštiti podataka, članak 8. stavak 1. druga alineja.

372 *Ibid.*, uvodna izjava 38.

373 *Ibid.*, uvodna izjava 58. Vidjeti i moderniziranu Konvenciju br. 108, članak 15. stavak 2. točka (e). Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavci 68. i 125.

374 Opća uredba o zaštiti podataka, članak 7. stavak 3.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 45.

375 Opća uredba o zaštiti podataka, članak 7. stavak 3.

376 Opća uredba o zaštiti podataka, uvodna izjava 42.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 42.

Primjer: Kupac pristane na primanje promidžbenih poruka na adresu koju je dostavio voditelju obrade podataka. Povučte li kupac privolu, voditelj obrade mora odmah prestati sa slanjem takvih promidžbenih poruka. Ne smiju se nametati nikakve kaznene mjere poput naknada. Povlačenje se odnosi na budućnost i nema retroaktivan učinak. Razdoblje u kojemu su se osobni podaci kupca zakonito obrađivali bilo je legitimno zahvaljujući privoli kupca. Povlačenjem se sprečava svaka daljnja obrada tih podataka, osim ako ta obrada nije u skladu s pravom na brisanje³⁷⁷.

Nužnost za izvršavanje ugovora

Prema pravu EU-a, člankom 6. stavkom 1. točkom (b) OUZP-a utvrđuje se dodatna osnova za zakonitu obradu, a to je da je obrada „nužna za izvršavanje ugovora u kojem je ispitanik stranka“. Ta odredba obuhvaća i predugovorne odnose. Na primjer, u slučajevima u kojima stranka namjerava sklopiti ugovor, no to još nije učinila, možda jer je potrebno obaviti još neke provjere. Ako jedna stranka treba obraditi podatke u tu svrhu, takva je obrada zakonita sve dok je nužna „kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora“³⁷⁸.

Ideja obrade podataka kao „legitimne osnove propisane zakonom“ iz članka 5. stavka 2. modernizirane Konvencije br. 108 također obuhvaća „obradu podataka u svrhu izvršavanja ugovora (ili predugovornih mjera na zahtjev osobe čiji se podaci obrađuju) u kojima je ispitanik stranka“³⁷⁹.

Pravne dužnosti voditelja obrade

U pravu EU-a utvrđuje se još jedna osnova za postizanje zakonitosti obrade podataka, i to ako je obrada „nužna radi poštovanja pravnih obveza voditelja obrade“ (članak 6. stavak 1. točka (c) OUZP-a). Ova se odredba odnosi na voditelje obrade koji djeluju i u privatnom i u javnom sektoru. Pravne obveze voditelja obrade iz javnog sektora također mogu potpadati pod članak 6. stavak 1. točku (e) OUZP-a. Mnogo je slučajeva u kojima su voditelji obrade iz privatnog sektora zakonom obvezani

377 Opća uredba o zaštiti podataka, članak 17. stavak 1. točka (b).

378 *Ibid.*, članak 6. stavak 1. točka (b).

379 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 46., Vijeće Europe, Odbor ministara (2010.), Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila, 23. studenoga 2010., članak 3.4. točka (b).

obrađivati podatke o pojedinim ispitanicima. Primjerice, poslodavci moraju obrađivati podatke o svojim zaposlenicima za potrebe socijalnog osiguranja i oporezivanja, a poduzeća moraju obrađivati podatke o svojim klijentima radi oporezivanja.

Pravna obveza može proizlaziti iz prava Unije ili države članice, koje može biti osnova za jedan ili više postupaka obrade. Zakonom se trebaju utvrditi svrha obrade, specifikacije za utvrđivanje voditelja obrade, vrste osobnih podataka koji podliježu obradi, dotičnih ispitanika, subjekata kojima se osobni podaci mogu otkriti, ograničenja svrhe, razdoblja pohrane i drugih mjera za osiguravanje zakonite i poštene obrade³⁸⁰. Svaki takav zakon koji predstavlja osnovu za obradu podataka mora biti u skladu s člancima 7. i 8. Povelje i člankom 8. EKLJP-a.

Pravne obveze voditelja obrade osnova su za zakonitu obradu podataka i unutar **prava Vijeća Europe**³⁸¹. Kao što je prethodno navedeno, pravne obveze voditelja obrade iz privatnog sektora samo su jedan poseban slučaj legitimnih interesa drugih, kao što je navedeno u članku 8. stavku 2. EKLJP-a. Stoga je primjer u kojemu poslodavci obrađuju osobne podatke zaposlenika relevantan i za pravo Vijeća Europe.

Vitalni interesi ispitanika ili druge fizičke osobe

Prema pravu EU-a, člankom 6. stavkom 1. točkom (d) OUZP-a propisuje se da je obrada osobnih podataka zakonita ako je „nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe”. Ta se legitimna osnova može primijeniti samo na obradu osobnih podataka na temelju životno važnih interesa druge fizičke osobe ako se takva obrada „očito ne može temeljiti na drugoj pravnoj osnovi”³⁸². Ponekad se vrsta obrade može temeljiti na osnovi javnog interesa i vitalnih interesa ispitanika ili druge osobe. Primjerice, to je slučaj pri praćenju epidemija i njihova razvoja ili kod pojave humanitarne krize.

Unutar prava Vijeća Europe vitalni interesi ispitanika ne spominju se u članku 8. EKLJP-a. Međutim, smatra se da se vitalni interesi ispitanika podrazumijevaju u sklopu pojma „legitimne osnove” iz članka 5. stavka 2. modernizirane Konvencije br. 108, koji se odnosi na legitimnost obrade osobnih podataka³⁸³.

380 Opća uredba o zaštiti podataka, uvodna izjava 45.

381 Vijeće Europe, Odbor ministara (2010.), Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila, 23. studenoga 2010., članak 3.4. točka (a).

382 Opća uredba o zaštiti podataka, uvodna izjava 46.

383 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 46.

Javni interes i izvršavanje javne ovlasti

S obzirom na to da se javni poslovi mogu organizirati na mnoge načine, člankom 6. stavkom 1. točkom (e) OUZP-a propisano je da se osobni podaci mogu zakonito obraditi ako je obrada „nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade”³⁸⁴.

Primjer: U predmetu *Huber protiv Bundesrepublik Deutschland*³⁸⁵ g. Huber, austrijski državljani s prebivalištem u Njemačkoj, zatražio je od Saveznog ureda za migracije i izbjeglice da izbriše podatke o njemu iz Središnjeg registra stranih državljana (AZR). Taj se registar, u kojemu su sadržani osobni podaci o stanovnicima Europske unije koji nisu njemački državljani, ali borave u Njemačkoj dulje od tri mjeseca, rabi u statističke svrhe i upotrebljavaju ga policijska i pravosudna tijela u istrazi i progonu kriminalnih aktivnosti ili aktivnosti koje ugrožavaju javnu sigurnost. Sud koji je prosljedio predmet postavio je pitanje je li obrada osobnih podataka koju obavlja registar poput Središnjeg registra stranih državljana, kojemu mogu pristupiti i druga javna tijela, sukladan s pravom Unije s obzirom na to da takav registar ne postoji za njemačke državljane.

SEU je smatrao da se prema članku 7. točki (e) Direktive 95/46/EZ³⁸⁶ osobni podaci mogu zakonito obrađivati ako je to nužno za izvršavanje zadatka koji se provodi zbog javnog interesa ili pri izvršavanju javne ovlasti.

Prema mišljenju SEU-a, „u pogledu cilja osiguranja jednake razine zaštite u svim državama članicama, [...] pojam potrebe, onako kako proizlazi iz članka 7. točke (e) Direktive 95/46/EZ³⁸⁷, ne može imati različit sadržaj ovisno o državama članicama. Iz toga proizlazi da se radi o pojmu koji ima vlastito neovisno značenje u pravu Zajednice i koji treba tumačiti na način kojim se u potpunosti održava cilj te direktive, kako je naveden u njezinu članku 1. stavku 1.”³⁸⁸.

384 Vidjeti Opću uredbu o zaštiti podataka, uvodna izjava 45.

385 SEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008.

386 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (e), sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (e).

387 *Ibid.*

388 SEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008., t. 52.

SEU je napomenuo da pravo na slobodu kretanja građana Unije na području države članice čiji nisu državljani nije bezuvjetno, već može podlijegati ograničenjima i uvjetima utvrđenima u Ugovoru o osnivanju Europske zajednice i mjerama donesenima radi njegove provedbe. Dakle, ako je, u načelu, zakonito da država članica upotrebljava registar poput AZR-a radi podrške tijelima odgovornima za primjenu zakonodavstva povezanog s pravom boravka, takav registar ne smije sadržavati informacije koje nisu nužne za tu određenu svrhu. SEU je zaključio da je takav sustav obrade osobnih podataka u skladu s pravom EU-a ako sadržava samo one podatke koji su potrebni za primjenu tog zakonodavstva i ako je zbog njegove centralizirane naravi primjena tog zakonodavstva učinkovitija. Nacionalni sud mora utvrditi jesu li ti uvjeti ispunjeni u ovom konkretnom slučaju. Ako nisu, pohrana i obrada osobnih podataka u registru poput AZR-a u statističke svrhe ne mogu se ni po kojoj osnovi smatrati nužnima u smislu članka 7. točke (e)³⁸⁹ Direktive 95/46/EZ³⁹⁰.

Naposljetku, što se tiče pitanja uporabe podataka sadržanih u registru u svrhu suzbijanja kriminala, SEU je smatrao da taj cilj „nužno uključuje progon počinjenih zločina ili kaznenih djela, neovisno o državljanstvu počinitelja”. Predmetni registar ne sadržava osobne podatke povezane s državljanima predmetne države članice i ta razlika u postupanju predstavlja diskriminaciju koja je zabranjena člankom 18. UFEU-a. Stoga je SEU zaključio da se tom odredbom, „isključuje mogućnost da država članica, u svrhu suzbijanja kriminala, uspostavi sustav za obradu osobnih podataka posebno za stanovnike Unije koji nisu državljani te države članice”³⁹¹.

Upotreba osobnih podataka od strane tijela koja djeluju u javnoj sferi također podliježe članku 8. **EKLJP-a** te je predviđeno da bude obuhvaćena člankom 5. stavkom 2. modernizirane Konvencije br. 108. kada je to primjenjivo³⁹².

389 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (e), sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (e).

390 SEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008., t. 54., 58., 59. i od 66. do 68.

391 *Ibid.*, t. 78. i 81.

392 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavci 46. i 47.

Legitimni interesi voditelja obrade ili treće strane

Prema **pravu EU-a**, ispitanik nije jedini koji ima legitimne interese. Člankom 6. stavkom 1. točkom (f) OUZP-a propisano je da se podaci mogu zakonito obraditi ako je obrada „nužna za potrebe legitimnih interesa voditelja obrade ili treće strane [osim tijela javne vlasti pri izvršavanju njihovih zadaća, kojima se podaci otkrivaju], osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu [...]”³⁹³.

Postojanje legitimnog interesa mora se pažljivo procijeniti u svakom pojedinom slučaju³⁹⁴. Ako se utvrde legitimni interesi voditelja obrade, mora se provesti postupak odvagivanja tih interesa i interesa ili temeljnih prava i sloboda ispitanika³⁹⁵. Tijekom takve procjene u obzir se moraju uzeti razumna očekivanja ispitanika kako bi se utvrdilo nadvladavaju li interesi voditelja obrade interese ili temeljna prava ispitanika³⁹⁶. Ako prava ispitanika nadvladavaju legitimne interese voditelja obrade, voditelj obrade može poduzeti određene mjere i primijeniti zaštitne mjere kako bi osigurao što manji učinak na prava ispitanika (kao što je pseudonimizacija podataka) te preokrenuti „ravnotežu” prije nego što se bude mogao zakonito osloniti na tu legitimnu osnovu obrade. U Mišljenju o pojmu legitimnih interesa voditelja obrade podataka, Radna skupina iz članka 29. istaknula je ključnu ulogu odgovornosti i transparentnosti te prava ispitanika na prigovor na obradu svojih podataka, ili na pristup tim podacima, njihovu izmjenu, brisanje ili prijenos, u odvagivanju legitimnih interesa voditelja obrade i interesa temeljnih prava ispitanika³⁹⁷.

U uvodnim izjavama OUZP-a pružaju se primjeri onoga što čini legitimni interes dotičnog voditelja obrade podataka. Primjerice, obrada osobnih podataka dopuštena je bez privole ispitanika kada se vrši u svrhe izravnog marketinga ili kada je takva obrada „nužna u svrhe sprečavanja prijevara”³⁹⁸.

U svojoj je sudskoj praksi SEU proširio procjenu kojom se utvrđuje što čini legitimni interes.

393 U odnosu na Direktivu 95/46/EZ, u Općoj uredbi o zaštiti podataka pruža se više primjera slučajeva za koje se smatra da predstavljaju legitimni interes.

394 Opća uredba o zaštiti podataka, preambula, uvodna izjava 47.

395 Radna skupina iz članka 29. (2014.), *Mišljenje 06/2014 o pojmu legitimnih interesa voditelja obrade podataka u skladu s člankom 7. Direktive 95/46/EZ*, WP 217, 4. travnja 2014.

396 *Ibid.*

397 *Ibid.*

398 Opća uredba o zaštiti podataka, preambula, uvodna izjava 47.

Primjer: Predmet *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*³⁹⁹ odnosio se na štetu koju je putnik naglim otvaranjem vrata taksija nanio trolejbusu prijevozničkog poduzeća u gradu Rigi. Društvo Rīgas satiksme htjelo je tužiti putnika taksija radi dobivanja odštete. Međutim, policija je pružila samo ime putnika te je uskratila njegov identifikacijski broj i adresu tvrdeći da bi takvo otkrivanje podataka bilo nezakonito prema nacionalnim zakonima o zaštiti podataka.

Latvijski sud koji je prosljedio predmet zatražio je da SEU donese prethodnu odluku o tome nameće li se zakonodavstvom EU-a o zaštiti podataka obveza priopćavanja svih osobnih podataka potrebnih za pokretanje građanske parnice protiv osobe koja je navodno odgovorna za počinjenje upravnog prekršaja⁴⁰⁰.

SEU je obrazložio da se zakonodavstvom EU-a o zaštiti podataka propisuje mogućnost – a ne obveza – priopćavanja podataka trećim stranama radi ostvarenja njihovih zakonitih interesa⁴⁰¹. SEU je utvrdio tri kumulativna uvjeta koji se moraju ispuniti kako bi obrada osobnih podataka bila zakonita na osnovi „zakonitih interesa”⁴⁰². Prvo, treća strana kojoj se podaci otkrivaju mora imati zakonit interes. U ovom konkretnom slučaju to znači da traženje osobnih podataka radi tuženja osobe zbog štete na imovini predstavlja zakonit interes treće strane. Drugo, obrada osobnih podataka mora biti nužna za ostvarenje tih zakonitih interesa. U ovom je slučaju ishođenje osobnih podataka kao što su adresa i/ili identifikacijski broj strogo nužno za identifikaciju dotične osobe. Treće, temeljna prava i slobode ispitanika ne smiju imati prednost nad zakonitim interesima voditelja obrade ili trećih strana. Odvagivanje interesa mora se provesti za svaki pojedini slučaj, uzimajući u obzir elemente poput težine kršenja prava ispitanika ili čak dobi ispitanika u određenim okolnostima. Međutim, u ovom slučaju SEU nije smatrao da je odbijanje otkrivanja podataka opravdano isključivo zbog činjenice da je ispitanik maloljetan.

399 SEU, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIa „Rīgas satiksme”*, 4. svibnja 2017.

400 *Ibid.*, t. 23.

401 *Ibid.*, t. 26.

402 *Ibid.*, t. od 28. do 34.

U predmetu *ASNEF i FECEMD* SEU je presudu donio isključivo o obradi podataka na temelju zakonite osnove „legitimnih interesa“, koja je u to vrijeme bila utvrđena u članku 7. točki (f) Direktive o zaštiti podataka⁴⁰³.

Primjer: U predmetu *ASNEF i FECEMD*⁴⁰⁴ SEU je pojasnio da se u nacionalnom zakonodavstvu ne smiju dodavati uvjeti onima navedenima u članku 7. točki (f) Direktive za zakonitu obradu podataka⁴⁰⁵. To se odnosilo na situaciju u kojoj je španjolski zakon o zaštiti podataka sadržavao odredbu na temelju koje bi druge privatne stranke mogle tvrditi da imaju legitiman interes u obradi osobnih podataka samo ako su se informacije već pojavile u javnim izvorima.

SEU je prvo napomenuo da je cilj Direktive 95/46/EZ⁴⁰⁶ osigurati jednaku razinu zaštite prava i sloboda pojedinaca u vezi s obradom osobnih podataka u svim državama članicama. Osim toga, usklađivanjem nacionalnih zakonodavstava primjenjivih u tom području ne smije se umanjiti razina zaštite. Naprotiv, njima se mora nastojati osigurati visoka razina zaštite u EU-u⁴⁰⁷. Stoga je SEU zaključio da „iz cilja osiguravanja jednake razine zaštite u svim državama članicama proizlazi da se člankom 7. Direktive 95/46/EZ⁴⁰⁸ navodi iscrpan i ograničen popis slučajeva u kojima je obradu osobnih podataka moguće smatrati zakonitom“. Osim toga, „države članice ne mogu dodavati nova načela koja se odnose na zakonitost obrade osobnih podataka u članak 7. Direktive 95/46/EZ⁴⁰⁹ niti nametati dodatne zahtjeve koji djeluju na način da izmjenjuju opseg primjene jednog od šest načela“ iz članka 7.

403 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (f), sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (f).

404 SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. studenoga 2011.

405 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (f), sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (f).

406 Nekadašnja Direktiva o zaštiti podataka, sada Opća uredba o zaštiti podataka.

407 SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. studenoga 2011., t. 28. Vidjeti Direktivu o zaštiti podataka, uvodne izjave 8. i 10.

408 Nekadašnja Direktiva o zaštiti podataka, članak 7., sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (f).

409 Nekadašnja Direktiva o zaštiti podataka, članak 7., sada Opća uredba o zaštiti podataka, članak 6.

Direktive⁴¹⁰. SEU je potvrdio da je u pogledu odvagivanja koje je potrebno prema članku 7. točki (f) Direktive 95/46/EZ moguće uzeti u obzir činjenicu da se ozbiljnost povrede temeljnih prava ispitanika koja proizlaze iz obrade može razlikovati ovisno o tome pojavljuju li se predmetni podaci već u javnim izvorima.

Međutim, prema članku 7. točki (f) Direktive „nije moguće da država članica kategorički i općenito isključi mogućnost obrade određenih kategorija osobnih podataka, a da pri tome ne omogući uzajamno uravnoteženje predmetnih suprotnih prava i interesa u konkretnom slučaju”.

S obzirom na navedeno, SEU je zaključio da članak 7. točku (f) Direktive 95/46/EZ⁴¹¹ treba tumačiti kao da „isključuje nacionalna pravila koja, u slučaju nepostojanja suglasnosti ispitanika, a radi omogućavanja obrade osobnih podataka ispitanika koja je nužna da bi se ispunili legitimni interesi voditelja obrade ili treće strane ili trećih strana kojima se ti podaci otkrivaju, iziskuju ne samo poštovanje temeljnih prava i sloboda ispitanika već i pojavljivanje podataka u javnim izvorima. Na taj se način kategorički i općenito isključuje obrada podataka koji se ne pojavljuju u takvim izvorima”⁴¹².

Kad god se osobni podaci obrađuju na temelju osnove „legitimnih interesa”, pojedinac ima pravo prigovora na obradu u svakom trenutku na osnovi povezanosti s njegovim konkretnim slučajem, u skladu s člankom 21. stavkom 1. OUZP-a. Voditelj obrade mora obustaviti obradu, osim ako uvjerljivo dokaže postojanje legitimne osnove za njezin nastavak.

Kad je riječ o **pravu Vijeća Europe**, slične se formulacije mogu pronaći u moderniziranoj Konvenciji br. 108⁴¹³ i preporukama Vijeća. U Preporuci o izradi profila potvrđuje se da je obrada osobnih podataka u svrhe izrade profila zakonita ako je nužna radi legitimnih interesa drugih, „osim kada su ti interesi podređeni temeljnim

410 *Ibid.*

411 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (f), sada Opća uredba o zaštiti podataka, članak 6. stavak 1. točka (f).

412 SEU, spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. studenoga 2011., t. 40., 44., 48. i 49.

413 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 46.

pravima i slobodama ispitanika⁴¹⁴. Usto, „zaštita prava i sloboda drugih” spominje se u članku 8. stavku 2. EKLP-a kao jedna od legitimnih osnova za ograničenje prava na zaštitu podataka.

Primjer: U predmetu *Y protiv Turske*⁴¹⁵ tužitelj je bio HIV pozitivan. Budući da je bio onesviješten pri dolasku u bolnicu, osoblje hitne pomoći obavijestilo je osoblje bolnice da je on HIV pozitivan. Tužitelj je pred ESLJP-om tvrdio da je otkrivanjem tih informacija prekršeno njegovo pravo na poštovanje privatnog života. Međutim, uzimajući u obzir potrebu za zaštitom sigurnosti bolničkog osoblja, dijeljenje tih informacija nije se smatralo kršenjem njegovih prava.

4.1.2. Obrada posebnih kategorija podataka (osjetljivih podataka)

Prema pravu Vijeća Europe, nacionalnim se zakonodavstvom utvrđuju odgovarajuće zaštite za uporabu osjetljivih podataka, pod uvjetom da su ispunjeni uvjeti iz članka 6. modernizirane Konvencije br. 108., prvenstveno da su odgovarajuće zaštitne mjere koje nadopunjuju druge odredbe Konvencije propisane zakonom. **Pravo Unije**, tj. članak 9. OUZP-a, sadržava detaljan režim obrade posebnih kategorija podataka (koji se nazivaju i „osjetljivim podacima”). To su podaci kojima se otkriva rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, a uključuju i genetske podatke, biometrijske podatke za potrebe jedinstvene identifikacije pojedinca, podatke koji se odnose na zdravlje, spolni život ili seksualnu orijentaciju pojedinca. Obrada osjetljivih podataka u načelu je zabranjena⁴¹⁶.

414 Vijeće Europe, Odbor ministara (2010.), *Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling* (Preporuka CM/Rec(2010)13 i Memorandum s objašnjenjima o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila), 23. studenoga 2010., članak 3.4. točka (b) (Preporuka o izradi profila).

415 ESLJP, *Y protiv Turske*, br. 648/10, 17. veljače 2015.

416 Nekadašnja Direktiva o zaštiti podataka, članak 7. točka (f), sada Opća uredba o zaštiti podataka, članak 9. stavak 1.

Međutim, u članku 9. stavku 2. Uredbe postoji iscrpan popis izuzeća od te zabrane, koja čine zakonite osnove za obradu osjetljivih podataka. Ta izuzeća uključuju sljedeće situacije:

- ispitanik dâ izričitu privolu za obradu podataka,
- obradu provodi neprofitno tijelo s političkim, filozofskim, vjerskim ili sindikalnim ciljem u sklopu svojih legitimnih aktivnosti te se ona odnosi samo na (bivše) članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s takvim svrhama,
- obrada se odnosi na osobne podatke koje je izričito objavio ispitanik,
- obrada je nužna:
 - za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u kontekstu zaposlenja, socijalne sigurnosti te socijalne zaštite,
 - za zaštitu životno važnih interesa ispitanika ili druge fizičke osobe (kada ispitanik nije u mogućnosti dati privolu),
 - za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu,
 - u svrhu preventivne medicine ili medicine rada: „radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava Unije ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom”,
 - za potrebe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe,
 - u svrhu javnog interesa u području javnog zdravlja, ili
 - za potrebe značajnog javnog interesa.

Stoga se za obradu posebnih kategorija podataka ugovorni odnos s ispitanikom ne smatra pravnom osnovom za zakonitu obradu osjetljivih podataka, osim ugovora sa zdravstvenim radnikom koji je obavezan čuvati profesionalnu tajnu⁴¹⁷.

Izričita privola ispitanika

Prema **pravu Unije**, prvi uvjet za zakonitu obradu bilo kojih podataka, neosjetljivih ili osjetljivih, privola je ispitanika. U slučaju osjetljivih podataka privola mora biti izričita. Međutim, zakonodavstvom Unije ili pojedinih država članica može se propisati da pojedinac ne smije ukinuti zabranu obrade posebnih kategorija podataka⁴¹⁸. Primjerice, to može vrijediti u slučaju kada obrada uključuje neuobičajene rizike za ispitanika.

Radno pravo ili pravo o socijalnoj sigurnosti i socijalnoj zaštiti

Prema **pravu Unije**, zabrana iz članka 9. stavka 1. može se ukinuti ako je obrada nužna za izvršavanje obveza ili ostvarivanje prava voditelja obrade ili ispitanika u području zaposlenja ili socijalne sigurnosti. Međutim, obrada mora biti odobrena u okviru prava Unije, nacionalnog prava ili kolektivnog ugovora u skladu s nacionalnim pravom, koji pružaju odgovarajuće zaštitne mjere za temeljna prava i interese ispitanika⁴¹⁹. Evidencija o zaposlenju koju vodi neka organizacija može sadržavati osjetljive osobne podatke koji su u određenim uvjetima utvrđeni u OUZP-u i relevantnom nacionalnom pravu. Primjeri osjetljivih podataka mogu uključivati članstvo u sindikatu ili zdravstvene informacije.

Vitalni interesi ispitanika ili druge osobe

Prema **pravu EU-a** osjetljivi podaci mogu se, kao i neosjetljivi podaci, obrađivati zbog vitalnih interesa ispitanika ili druge fizičke osobe⁴²⁰. Kada se obrada temelji na vitalnim interesima druge osobe, ta zakonita osnova može se primijeniti samo ako se takva obrada „očito ne može temeljiti na drugoj pravnoj osnovi“⁴²¹. U nekim slučajevima obradom osobnih podataka mogu se zaštititi javni i privatni interesi, primjerice kada je obrada potrebna u humanitarne svrhe⁴²².

417 Opća uredba o zaštiti podataka, članak 9. stavak 2. točke (h) i (i).

418 *Ibid.*, članak 9. stavak 2. točka (a).

419 *Ibid.*, članak 9. stavak 2. točka (b).

420 *Ibid.*, članak 9. stavak 2. točka (c).

421 *Ibid.*, uvodna izjava 46.

422 *Ibid.*

Da bi obrada osjetljivih podataka bila zakonita na toj osnovi, traženje privole od ispitanika mora biti onemogućeno, primjerice jer je ispitanik u nesvijesti ili odsutan i nedostupan. Drugim riječima, ta osoba mora biti fizički ili pravno nesposobna za davanje privole.

Humanitarne udruge ili neprofitna tijela

Obrada osobnih podataka dopuštena je i u sklopu legitimnih aktivnosti zaklada, udruženja ili drugih neprofitnih tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem. Međutim, obrada se mora odnositi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s tijelom⁴²³. Osjetljivi podaci ne smiju se otkrivati izvan tih tijela bez privole ispitanika.

Podaci koje očito objavljuje ispitanik

U članku 9. stavku 2. točki (e) OUZP-a navodi se da obrada nije zabranjena ako se odnosi na podatke za koje je očito da ih je objavio ispitanik. Iako značenje izraza „očito da ih je objavio ispitanik” nije definirano u Uredbi, budući da se radi o izuzeću od zabrane obrade osjetljivih podataka, mora se strogo tumačiti tako da se od ispitanika zahtijeva da s namjerom objavi svoje osobne podatke. Stoga kada se u sklopu televizijskog prijenosa prikaže videozapis snimljen kamerom videonadzora koji, među ostalim, pokazuje vatrogasca koji zadobiva ozljede prilikom evakuacije zgrade, ne može se reći da je taj vatrogasac očito objavio svoje podatke. S druge strane, ako taj vatrogasac odluči opisati događaj i objaviti videozapis i fotografije na javnoj internetskoj stranici, morao bi poduzeti svjestan, potvrđan čin kako bi objavio osobne podatke. Važno je napomenuti da objava vlastitih podataka ne predstavlja privolu, nego još jedno dopuštenje za obradu posebnih kategorija podataka.

Činjenica da je ispitanik objavio obrađene osobne podatke ne oslobađa voditelje obrade od njihovih obveza na temelju zakonodavstva o zaštiti podataka. Primjerice, načelo ograničenja svrhe primjenjuje se na osobne podatke čak i ako takvi podaci postanu javno dostupni⁴²⁴.

423 *Ibid.*, članak 9. stavak 2. točka (d).

424 Radna skupina iz članka 29. (2013.), *Opinion 3/2013 on purpose limitation* (Mišljenje 3/2013 o ograničavanju svrhe), WP 203, Bruxelles, 2. travnja 2013., str. 14.

Pravni zahtjevi

Obrada posebnih kategorija podataka koja je „nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva”, neovisno o tome je li riječ o parničnom, upravnom ili izvanparničnom postupku,⁴²⁵ također je dopuštena OUZP-om⁴²⁶. U tom slučaju obrada mora biti relevantna za pojedini pravni zahtjev, odnosno njegovo ostvarivanje ili obranu, a može je zatražiti bilo koja od stranaka u sporu.

Kad sudovi djeluju u sudbenom svojstvu, mogu obrađivati posebne kategorije podataka u kontekstu rješavanja pravnog spora⁴²⁷. Te posebne kategorije podataka koji se obrađuju u ovom kontekstu mogu uključivati, primjerice, genetske podatke prilikom utvrđivanja roditeljstva ili zdravstveno stanje kada se dio dokaza odnosi na pojedinosti o ozljedama koje zadobije žrtva kaznenog djela.

Razlozi značajnog javnog interesa

Prema članku 9. stavku 2. točki (g) OUZP-a, države članice mogu propisati dodatne okolnosti u kojima se osjetljivi podaci mogu obrađivati:

- ako je obrada podataka potrebna zbog značajnog javnog interesa,
- ako je to propisano europskim ili nacionalnim pravom,
- ako je europsko ili nacionalno pravo razmjerno te se njime poštuje pravo na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu prava i interesa ispitanika⁴²⁸.

Dobar su primjer elektronički sustavi zdravstvenih kartona. Takvi sustavi omogućuju dostupnost zdravstvenih podataka koje prikupljaju zdravstveni radnici tijekom liječenja pacijenta drugim zdravstvenim radnicima tog pacijenta na širokoj osnovi, najčešće nacionalnoj.

⁴²⁵ Opća uredba o zaštiti podataka, preambula, uvodna izjava 52.

⁴²⁶ *Ibid.*, članak 9. stavak 2. točka (f).

⁴²⁷ *Ibid.*

⁴²⁸ *Ibid.*, članak 9. stavak 2. točka (g).

Radna skupina iz članka 29. zaključila je da do uspostave takvih sustava ne bi moglo doći prema postojećim zakonskim propisima za obradu podataka o pacijentima⁴²⁹. Međutim, elektronički sustavi zdravstvenih kartona mogu postojati ako se temelje na „potrebama značajnog javnog interesa“⁴³⁰. Za njihovu bi uspostavu bila potrebna izričita pravna osnova, koja bi uključivala i potrebne zaštitne mjere za siguran rad sustava⁴³¹.

Ostale osnove za obradu osjetljivih podataka

OUZP-om se propisuje da se osjetljivi podaci mogu obrađivati ako je obrada nužna u svrhu⁴³²:

- preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava EU-a ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom,
- javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda, na temelju prava EU-a ili prava države članice. Pravom se moraju propisati odgovarajuće i posebne mjere za zaštitu prava ispitanika,
- arhiviranja, znanstvenog ili povijesnog istraživanja ili u statističke svrhe na temelju prava EU-a ili prava države članice. Pravo mora biti razmjerno cilju koji se nastoji postići, njime se mora poštovati bit prava na zaštitu podataka i osiguravati prikladne i posebne mjere za zaštitu prava i interesa ispitanika.

429 Radna skupina iz članka 29. (2007.), *Working Document on the processing of personal data relating to health in electronic health records (EHR)* (Radni dokument o obradi osobnih podataka koji se odnose na zdravlje u elektroničkim zdravstvenim kartonima), WP 131, Bruxelles, 15. veljače 2007. Vidjeti i Opću uredbu o zaštiti podataka, članak 9. stavak 3.

430 Opća uredba o zaštiti podataka, članak 9. stavak 2. točka (g).

431 Radna skupina iz članka 29. (2007.), *Radni dokument o obradi osobnih podataka koji se odnose na zdravlje u elektroničkim zdravstvenim kartonima*, WP 131, Bruxelles, 15. veljače 2007.

432 Opća uredba o zaštiti podataka, članak 9. stavak 2. točke (h), (i) i (j).

Dodatni uvjeti na temelju nacionalnog zakonodavstva

OUZP-om se državama članicama također omogućuje da uvedu ili zadrže dodatne uvjete, uključujući ograničenja obrade genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje⁴³³.

4.2. Pravila sigurnosti obrade

Ključne točke

- Prema pravilima sigurnosti obrade, voditelj obrade i izvršitelj obrade obvezni su provesti odgovarajuće tehničke i organizacijske mjere kako bi spriječili neovlašteno ometanje postupaka obrade podataka.
- Nužna razina sigurnosti podataka određuje se prema:
 - sigurnosnim značajkama dostupnima na tržištu za određenu vrstu obrade,
 - troškovima,
 - rizicima obrade podataka za temeljna prava i slobode ispitanika.
- Osiguravanje povjerljivosti osobnih podataka dio je općih načela priznatih Općom uredbom o zaštiti podataka.

Prema **pravu EU-a i Vijeća Europe**, voditelji obrade imaju opću obvezu transparentnosti i odgovornosti pri obradi osobnih podataka, a posebno u pogledu povreda podataka kada do njih dođe. U slučaju povreda osobnih podataka voditelji obrade moraju izvijestiti nadzorna tijela, osim ako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca. Ispitanici također trebaju biti obaviješteni o povredi osobnih podataka kada će ona vjerojatno dovesti do visokog rizika za prava i slobode pojedinaca.

4.2.1. Elementi sigurnosti podataka

Prema odgovarajućim odredbama **prava EU-a**:

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti

⁴³³ *Ibid.*, članak 9. stavak 2. točka (h) i članak 9. stavak 4.

za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik [...]»⁴³⁴.

Te mjere, među ostalim, uključuju sljedeće:

- pseudonimizaciju i enkripciju osobnih podataka⁴³⁵,
- osiguravanje trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade⁴³⁶,
- pravodobnu ponovnu uspostavu dostupnosti osobnih podataka i pristupa njima u slučaju gubitka podataka⁴³⁷,
- proces za testiranje, ocjenjivanje i procjenjivanje učinkovitosti mjera za osiguravanje sigurnosti obrade⁴³⁸.

Unutar **prava Vijeća Europe** postoji slična odredba:

Svaka stranka osigurava da voditelj obrade i, kada je to primjenjivo, izvršitelj obrade, poduzimaju odgovarajuće sigurnosne mjere protiv rizika poput slučajnog ili neovlaštenog uništenja, gubitka, upotrebe, izmjene ili otkrivanja osobnih podataka ili pristupa njima»⁴³⁹.

Prema **pravu EU-a i Vijeća Europe**, u slučaju povrede podataka koja može utjecati na prava i slobode pojedinaca voditelj obrade dužan je o njoj obavijestiti nadzorno tijelo (vidjeti [dio 4.2.3.](#)).

Često su utvrđeni i industrijski, nacionalni i međunarodni standardi sigurne obrade podataka. Na primjer, Europski pečat za zaštitu podataka (EuroPriSe) projekt je transeuropske telekomunikacijske mreže (eTEN) Europske unije kojim se istražuju mogućnosti certificiranja proizvoda, naročito softvera, u svrhu usklađivanja

434 *Ibid.*, članak 32. stavak 1.

435 *Ibid.*, članak 32. stavak 1. točka (a).

436 *Ibid.*, članak 32. stavak 1. točka (b).

437 *Ibid.*, članak 32. stavak 1. točka (c).

438 *Ibid.*, članak 32. stavak 1. točka (d).

439 Modernizirana Konvencija br. 108, članak 7. stavak 1.

s europskim zakonodavstvom o zaštiti podataka. Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA) osnovana je radi unapređivanja sposobnosti Europske unije, država članica Europske unije i poslovne zajednice u pogledu sprečavanja, rješavanja i odgovaranja na probleme s mrežnom i informacijskom sigurnošću⁴⁴⁰. ENISA redovito izdaje analize trenutanih sigurnosnih prijetnji i savjete o njihovu rješavanju⁴⁴¹.

Sigurnost podataka ne postiže se samo primjenom prave opreme, odnosno hardvera i softvera. Ona ovisi i o odgovarajućim internim organizacijskim pravilima. Takvim bi internim pravilima, idealno, bila obuhvaćena sljedeća pitanja:

- redovito pružanje informacija svim zaposlenicima o pravilima sigurnosti podataka i njihovim obvezama prema zakonodavstvu o zaštiti podataka, naročito u pogledu njihovih obveza povjerljivosti,
- jasna raspodjela odgovornosti i jasan prikaz stručnih vještina u području obrade podataka, naročito u pogledu odluka o obradi osobnih podataka i prijenosa podataka trećim stranama ili ispitanicima,
- upotreba podataka samo prema uputama nadležne osobe ili prema općenito utvrđenim pravilima,
- zaštita pristupa lokacijama i hardveru i softveru voditelja ili izvršitelja obrade, uključujući provjere ovlaštenja za pristup,
- osiguravanje da je ovlaštenja za pristup osobnim podacima dodijelila nadležna osoba i zahtijevanje odgovarajuće dokumentacije,
- automatizirani protokoli o pristupu osobnim podacima elektroničkim putem i redovite provjere takvih protokola koje provodi interna nadzorna služba (zbog čega je nužno da sve aktivnosti obrade podataka budu evidentirane),

440 Uredba (EZ) br. 526/2013 Europskog parlamenta i Vijeća od 21. svibnja 2013. o Agenciji Europske unije za mrežnu i informacijsku sigurnost (ENISA) i o stavljanju izvan snage Uredbe (EZ) br. 460/2004, SL 2013 L 165.

441 Primjerice, ENISA, (2016.), *Cyber Security and Resilience of smart cars. Good practices and recommendations* (Kibersigurnost i otpornost pametnih automobila: dobre prakse i preporuke); ENISA (2016.), *Security of Mobile Payments and Digital Wallets* (Sigurnost mobilnog plaćanja i digitalnih novčanika).

- pažljivo dokumentiranje drugih oblika otkrivanja osim automatiziranog pristupa podacima kako bi se moglo dokazati da nije došlo ni do kakvih nezakonitih prijenosa podataka.

Ponuda odgovarajuće obuke i obrazovanja o sigurnosti podataka članovima osoblja također je važan element učinkovitih sigurnosnih mjera opreza. Također je potrebno uspostaviti postupke provjere kako bi se osiguralo da odgovarajuće mjere ne postoje samo na papiru nego da se provode i djeluju i u praksi (kao što su unutarnje ili vanjske revizije).

Mjere za poboljšanje razine sigurnosti voditelja ili izvršitelja obrade uključuju instrumente kao što su službenici za zaštitu osobnih podataka, obrazovanje zaposlenika o sigurnosti, redovne revizije, ispitivanja probojnosti i pečati kvalitete.

Primjer: U predmetu *I. protiv Finske*⁴⁴² tužiteljica nije uspjela dokazati da su drugi zaposlenici bolnice u kojoj je radila nezakonito pristupili njezinu zdravstvenom kartonu. Stoga su nacionalni sudovi odbacili njezinu tužbu zbog povrede prava na zaštitu podataka. ESLJP je zaključio da je došlo do kršenja članka 8. EKLJP-a jer bolnički sustav evidencije zdravstvenih kartona „nije omogućio retroaktivno obrazloženje uporabe pacijentovih kartona s obzirom na to da je prikazivao samo pet posljednjih uvida i da su se te informacije brisale nakon vraćanja datoteke u arhivu“. Za ESLJP je od presudne važnosti bilo da bolnički evidencijski sustav očito nije bio u skladu sa zakonskim zahtjevima iz nacionalnog zakonodavstva, čemu nacionalni sudovi nisu pridali dovoljno važnosti.

Europska unija donijela je Direktivu o sigurnosti mrežnih i informacijskih sustava (NIS direktiva)⁴⁴³, prvi pravni instrument posvećen kibernetičkoj sigurnosti na razini EU-a. Direktivom se nastoji poboljšati kibernetička sigurnost na nacionalnoj razini te povećati razina suradnje unutar EU-a. Njome se također propisuju obveze za operatere ključnih usluga (uključujući operatere u energetskom, zdravstvenom, bankarskom i prometnom sektoru te sektoru digitalne infrastrukture) i pružatelje digitalnih usluga koje se odnose na upravljanje rizicima, osiguravanje sigurnosti njihovih mrežnih i informacijskih sustava te prijavu sigurnosnih incidenata.

442 ESLJP, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.

443 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL 2016 L 194.

Izgledi

U rujnu 2017. Europska komisija izradila je Prijedlog uredbe za reformu ovlasti ENISA-e kako bi se u obzir uzele nove ovlasti i odgovornosti te agencije na temelju NIS direktive. Cilj je Prijedloga uredbe razvijanje ENISA-inih zadataka i potvrda njezine uloge „referentne točke u kiberekosustavu EU-a”⁴⁴⁴. Prijedlogom uredbe ne smiju se u pitanje dovesti načela OUZP-a, a pojašnjavanjem nužnih elemenata koji čine europske programe kibersigurnosne certifikacije trebala bi se povećati sigurnost osobnih podataka. Istodobno, u rujnu 2017. Europska komisija izradila je Prijedlog provedbene uredbe kojom bi se utvrdili elementi koje pružatelji digitalnih usluga moraju uzeti u obzir kako bi zajamčili sigurnost svojih mrežnih i informacijskih sustava, kao što je propisano člankom 16. stavkom 8. Direktive o NIS-u. U vrijeme izrade ovog priručnika rasprave o tim dvama prijedlozima još su bile u tijeku.

4.2.2. Povjerljivost

Unutar prava EU-a OUZP-om se povjerljivost osobnih podataka utvrđuje kao dio općeg načela⁴⁴⁵. Pružatelji javno dostupnih elektroničkih komunikacijskih usluga moraju osigurati povjerljivost. Također imaju obvezu jamčiti sigurnost svojih usluga⁴⁴⁶.

Primjer: Zaposlenik osiguravajućeg društva na poslu primi telefonski poziv od osobe koja tvrdi da je klijent i traži podatke o svojem ugovoru o osiguranju.

S obzirom na to da je dužan podatke klijenata čuvati u tajnosti, zaposlenik mora primijeniti barem minimalne mjere sigurnosti prije otkrivanja osobnih podataka. Način na koji to može učiniti jest, na primjer, tako da ponudi uzvratiti poziv na telefonski broj zabilježen u klijentovu dosjeu.

Prema članku 5. stavku 1. točki (f), osobni podaci moraju se obrađivati na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera („cjelovitost i povjerljivost”).

444 Prijedlog uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti”), COM(2017)477, 13. rujna 2017., str. 6.

445 Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (f).

446 Direktiva o privatnosti i elektroničkim komunikacijama, članak 5. stavak 1.

Sukladno članku 32., voditelj obrade i izvršitelj obrade moraju provesti tehničke i organizacijske mjere za osiguravanje visoke razine sigurnosti. Takve mjere, među ostalim, uključuju pseudonimizaciju i enkripciju osobnih podataka, sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti obrade, ocjenjivanje i testiranje učinkovitosti mjera te sposobnost ponovne uspostave obrade podataka u slučaju fizičkog ili tehničkog incidenta. Osim toga, poštovanje odobrenog kodeksa ponašanja ili odobrenog mehanizma certificiranja može se iskoristiti kao element za dokazivanje sukladnosti s načelom cjelovitosti i povjerljivosti. Prema članku 28. OUZP-a, ugovorom kojim se izvršitelj obrade obvezuje prema voditelju obrade mora se odrediti da izvršitelj obrade osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu primjenjivim zakonskim obvezama o povjerljivosti.

Obveza povjerljivosti ne odnosi se na situacije u kojima osoba sazna za podatke u svojstvu privatnog pojedinca, a ne zaposlenika voditelja ili izvršitelja obrade. U tom se slučaju članci 32. i 28. OUZP-a ne primjenjuju jer je upotreba osobnih podataka koju provode privatni pojedinci potpuno izuzeta iz područja primjene Uredbe kada takva upotreba potpada u okviru takozvanog izuzeća za kućanstvo⁴⁴⁷. Izuzeće za kućanstvo odnosi se na upotrebu osobnih podataka „koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti”⁴⁴⁸. Nakon odluke SEU-a u predmetu *Bodil Lindqvist*⁴⁴⁹ to se izuzeće, međutim, treba usko tumačiti, naročito u pogledu otkrivanja podataka. Točnije, izuzeće za kućansku uporabu ne proširuje se na objavu osobnih podataka neograničenom broju primatelja na internetu ni na obradu podataka koja ima profesionalne ili komercijalne aspekte (za više pojedinosti o predmetu vidjeti [dijelove 2.1.2., 2.2.2. i 2.3.1.](#)).

„Povjerljivost komunikacija” još je jedan aspekt povjerljivosti koji podliježe *lex specialis*. Posebnim propisima za osiguravanje povjerljivosti elektroničkih komunikacija na temelju Direktive o privatnosti i elektroničkim komunikacijama državama članicama nalaže se da zabrane svim osobama koje nisu korisnici slušanje, prisluškivanje, pohranjivanje ili druge oblike presretanja odnosno nadzora nad komunikacijama i s time povezanim metapodacima bez pristanka korisnika⁴⁵⁰. Nacionalnim zakonodavstvom mogu se dopustiti izuzeća od tog načela isključivo kada je to nužno za nacionalnu sigurnost, obranu, sprečavanje ili otkrivanje kaznenih djela, te samo ako su

447 Opća uredba o zaštiti podataka, članak 2. stavak 2. točka (c).

448 *Ibid.*

449 SEU, C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003.

450 Direktiva o privatnosti i elektroničkim komunikacijama, članak 5. stavak 1.

takve mjere nužne i razmjerne ciljevima koji se nastoje postići⁴⁵¹. Isti će se propisi primjenjivati u sklopu buduće Uredbe o e-privatnosti, no područje primjene pravnog akta o e-privatnosti proširit će se s javno dostupnih elektroničkih komunikacijskih usluga na komunikacije putem „OTT usluga” (kao što su mobilne aplikacije).

Unutar prava Vijeća Europe obveza povjerljivosti podrazumijeva se u pojmu sigurnosti podataka iz članka 7. stavka 1. modernizirane Konvencije br. 108, u kojemu se obrađuje sigurnost podataka.

Za izvršitelje obrade povjerljivost znači da podatke ne smiju otkrivati trećim stranim ni drugim primateljima bez ovlaštenja. Za zaposlenike voditelja ili izvršitelja obrade povjerljivost znači da osobne podatke smiju upotrebljavati samo u skladu s uputama svojih nadležnih nadređenih osoba.

Obveza povjerljivosti mora biti sadržana u svakom ugovoru između voditelja obrade i njihovih izvršitelja obrade. Usto, voditelji obrade i izvršitelji obrade moraju poduzeti posebne mjere kako bi za svoje zaposlenike uspostavili pravnu obvezu povjerljivosti. To se obično postiže uključivanjem odredbi o povjerljivosti u ugovor o radu sa zaposlenikom.

Kršenje profesionalne obveze povjerljivosti kažnjivo je na temelju kaznenog prava u mnogim državama članicama EU-a i strankama Konvencije br. 108.

4.2.3. Obavješćivanje u slučaju povrede osobnih podataka

Povreda osobnih podataka odnosi se na povredu sigurnosti koja dovodi do nehotičnog ili nezakonitog uništenja, gubitka, izmjene ili neovlaštenog otkrivanja obrađenih osobnih podataka ili pristupa njima⁴⁵². Iako nove tehnologije poput šifriranja sada pružaju više mogućnosti za osiguravanje sigurnosti obrade, povrede podataka i dalje su česta pojava. Uzroci povreda podataka mogu biti razni, od nehotičnih pogrešaka koje počinu osobe koje rade unutar organizacije do vanjskih prijetnji poput hakera i organizacija koje se bave kiberkriminalom.

⁴⁵¹ *Ibid.*, članak 15. stavak 1.

⁴⁵² Opća uredba o zaštiti podataka, članak 4. stavak 12.; vidjeti i *Smjernice o obavješćivanju o povredi osobnih podataka na temelju Uredbe 2016/679*, Radne skupine iz članka 29. (2017.), WP 250, 3. listopada 2017., str. 8.

Povrede podataka mogu biti vrlo štetne za prava na privatnost i zaštitu podataka pojedinaca koji zbog takve povrede mogu izgubiti kontrolu nad svojim osobnim podacima. Povrede podataka mogu dovesti do krađe identiteta ili prijevare, financijskog gubitka ili materijalne štete, gubitka povjerljivosti osobnih podataka koji su zaštićeni poslovnom tajnom te narušavanja ugleda ispitanika. U Smjernicama o obavješćivanju o povredi osobnih podataka na temelju Uredbe (EU) 2016/679 Radna skupina iz članka 29. pojašnjava da povrede podataka mogu imati tri različite posljedice za osobne podatke: otkrivanje, gubitak i/ili izmjenu⁴⁵³. Uz obvezu poduzimanja mjera za osiguravanje sigurnosti obrade, kako je pojašnjeno u [dijelu 4.2.](#), jednako je važno osigurati da voditelji obrade u slučaju povrede podataka postupaju na odgovarajući način i pravovremeno.

Nadzorna tijela i pojedinci često nisu svjesni povrede podataka, zbog čega pojedinci ne mogu poduzeti potrebne korake da se zaštite od njezinih negativnih posljedica. Kako bi se potvrdila prava pojedinaca i ograničile posljedice povreda podataka, **EU i Vijeće Europe** u određenim okolnostima voditeljima obrade nalažu obvezu obavješćivanja.

Prema moderniziranoj Konvenciji br. 108 **Vijeća Europe**, ugovorne stranke moraju od voditelja obrade zahtijevati barem da obavijeste nadležno nadzorno tijelo o povredama podataka koje mogu ozbiljno omesti prava ispitanika. Takvo obavješćivanje mora se provesti „bez odgode”⁴⁵⁴.

Pravom EU-a utvrđuje se detaljan režim rokova i sadržaja obavijesti⁴⁵⁵. Voditelji obrade moraju obavijestiti nadzorna tijela o određenim povredama podataka bez nepotrebne odgode i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi. Ako se prekorači rok od 72 sata, obavješćivanje mora biti popraćeno obrazloženjem kašnjenja. Voditelji obrade izuzeti su od obveze obavješćivanja samo ako mogu dokazati da nije vjerojatno da će povreda podataka prouzročiti rizik za prava i slobode dotičnih pojedinaca.

Uredbom se utvrđuju minimalne informacije koje moraju biti uključene u obavijest kako bi nadzorno tijelo moglo poduzeti potrebne mjere.⁴⁵⁶ Obavijest mora sadržavati

453 Radna skupina iz članka 29. (2017.), *Smjernice o obavješćivanju o povredi osobnih podataka na temelju Uredbe 2016/679*, WP 250, 3. listopada 2017., str. 6.

454 Modernizirana Konvencija br. 108, članak 7. stavak 2.; Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavci od 64. do 66.

455 Opća uredba o zaštiti podataka, članci 33. i 34.

456 *Ibid.*, članak 33. stavak 3.

barem opis prirode povrede podataka i kategorije i približan broj ispitanika pogođenih povredom, opis vjerojatnih posljedica povrede te mjere koje je voditelj obrade poduzeo za rješavanje problema povrede i umanjivanje njezinih posljedica. Usto je potrebno navesti ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke kako bi nadležno nadzorno tijelo po potrebi moglo dobiti više informacija.

U slučaju povrede podataka koja će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebne odgode mora obavijestiti pojedince (ispitanike) o povredi⁴⁵⁷. Informacije pružene ispitanicima, uključujući opis povrede podataka, moraju biti napisane jasnim i jednostavnim jezikom te uključivati informacije slične onima koje su nužne pri obavješćivanju nadzornih tijela. U određenim okolnostima voditelji obrade mogu biti izuzeti od obveze obavješćivanja ispitanika o takvim povredama podataka. Izuzeća se primjenjuju kada je voditelj obrade poduzeo odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke zahvaćene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija. Voditelj obrade može biti oslobođen obveze obavješćivanja ispitanika i ako nakon povrede poduzme mjere osiguravanja da više ne dođe do visokog rizika za prava i slobode ispitanika. Naposljetku, ako obavješćivanje zahtijeva nerazmjeran napor za voditelja obrade, ispitanike se može obavijestiti o povredi podataka i na druge načine, poput javnog obavješćivanja ili sličnih mjera⁴⁵⁸.

Obveza obavješćivanja nadzornih tijela i ispitanika o povredama podataka odnosi se na voditelje obrade. Međutim, povrede podataka mogu se dogoditi neovisno o tome provodi li obradu voditelj obrade ili izvršitelj obrade. Zbog toga je neophodno osigurati da izvršitelji obrade također izvješćuju o povredama podataka. U tom slučaju izvršitelji obrade moraju obavijestiti voditelja obrade o povredama podataka bez nepotrebne odgode⁴⁵⁹. Voditelj obrade zatim je odgovoran za obavješćivanje nadzornih tijela i dotičnih ispitanika sukladno prethodno navedenim pravilima i rokovima.

457 *Ibid.*, članak 34.

458 *Ibid.*, članak 34. stavak 3. točka (c).

459 *Ibid.*, članak 33. stavak 2.

4.3. Propisi o odgovornosti i promicanju usklađenosti

Ključne točke

- Kako bi se osigurala odgovornost pri obradi osobnih podataka, voditelji obrade i izvršitelji obrade moraju voditi evidenciju o aktivnostima obrade koje se obavljaju pod njihovom odgovornošću i na zahtjev je predložiti nadzornim tijelima.
- U Općoj uredbi o zaštiti podataka utvrđuje se nekoliko instrumenata za postizanje sukladnosti:
 - imenovanje službenika za zaštitu podataka u određenim slučajevima,
 - provođenje procjene učinka prije početka aktivnosti obrade koje će vjerojatno uzrokovati visok rizik za prava i slobode pojedinaca,
 - prethodno savjetovanje s nadležnim nadzornim tijelom ako procjena učinka ukazuje na to da obrada donosi rizike koji se ne mogu umanjiti,
 - kodeksi ponašanja za voditelje obrade i izvršitelje obrade kojima se utvrđuje primjena Uredbe u pojedinim sektorima obrade,
 - mehanizmi certificiranja, pečati i oznake.
- U sklopu prava Vijeća Europe, odnosno modernizirane Konvencije br. 108, predlažu se slični instrumenti za postizanje sukladnosti.

Načelo odgovornosti posebno je važno za osiguravanje provedbe propisa o zaštiti podataka u Europi. Voditelj obrade odgovoran je za sukladnost s propisima o zaštiti podataka i mora je moći dokazati. Odgovornost ne bi smjela biti u prvom planu tek nakon kršenja propisa. Naprotiv, voditelji obrade imaju proaktivnu obvezu pridržavati se odgovarajućih pravila za upravljanje podacima u svim fazama obrade podataka. Europskim zakonodavstvom o zaštiti podataka voditelji obrade obavezuju se na provođenje tehničkih i organizacijskih mjera kojima će osigurati da se obrada provodi u skladu sa zakonom i dokazati tu sukladnost. Među tim su mjerama imenovanje službenika za zaštitu podataka, vođenje evidencije i dokumentacije u vezi s obradom te provođenje procjena učinka na privatnost.

4.3.1. Službenici za zaštitu podataka

Službenici za zaštitu podataka (SZP) osobe su koje pružaju savjete o sukladnosti s propisima o zaštiti podataka u organizacijama koje obavljaju obradu podataka. Oni su „temelj odgovornosti” jer pridonose sukladnosti te istovremeno djeluju kao posrednici između nadzornih tijela, ispitanika i organizacija koje ih imenuju.

Prema pravu Vijeća Europe, člankom 10. stavkom 1. modernizirane Konvencije br. 108 voditeljima obrade i izvršiteljima obrade propisuje se opća obveza odgovornosti. Od voditelja obrade i izvršitelja obrade zahtijeva se da poduzimaju sve odgovarajuće mjere za usklađenost s propisima o zaštiti podataka utvrđenima u Konvenciji te da su sposobni dokazati da je obrada podataka pod njihovim vodstvom u skladu s odredbama Konvencije. Iako u Konvenciji nisu utvrđene konkretne mjere koje voditelji obrade i izvršitelji obrade trebaju poduzeti, u Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da bi imenovanje SZP-a bila jedna od mogućih mjera za dokazivanje usklađenosti. SZP-ovi na raspolaganju trebaju imati sva potrebna sredstva kako bi ispunili svoje ovlasti⁴⁶⁰.

Za razliku od prava Vijeća Europe, **u EU-u** imenovanje SZP-a nije uvijek prepušteno odluci voditelja obrade i izvršitelja obrade, već je u određenim uvjetima i obavezno. U OUZP-u se službenik za zaštitu podataka smatra ključnom ulogom u novom sustavu upravljanja te se navode detaljne odredbe o imenovanju, funkciji, dužnostima i zadaćama tog službenika⁴⁶¹.

Prema OUZP-u, imenovanje službenika za zaštitu podataka obavezno je u trima posebnim slučajevima: kada obradu provodi tijelo javne vlasti ili javno tijelo, kada se osnovne djelatnosti voditelja ili izvršitelja obrade sastoje od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri ili kada se njihove osnovne djelatnosti sastoje od opsežne obrade posebnih kategorija podataka ili osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima⁴⁶². Iako pojmovi „sustavno praćenje u velikoj mjeri” i „osnovne djelatnosti” nisu definirani u Uredbi, Radna skupina iz članka 29. objavila je smjernice o njihovom tumačenju⁴⁶³.

460 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 87.

461 Opća uredba o zaštiti podataka, članci od 37. do 39.

462 *Ibid.*, članak 37. stavak 1.

463 Radna skupina iz članka 29. (2017.), *Smjernice o službenicima za zaštitu podataka („SZP-ovima”)*, WP 243 rev.01, posljednji put revidirane i donesene 5. travnja 2017.

Primjer: Društva koja upravljaju društvenim mrežama i internetskim tražilicama vjerojatno će se smatrati voditeljima obrade čiji postupci obrade zahtijevaju redovito i sustavno praćenje ispitanika u velikoj mjeri. Poslovni model takvih društava temelji se na obradi velikih količina osobnih podataka te ona ostvaruju znatan prihod od pružanja ciljanih marketinških usluga i omogućivanja drugim društvima da se oglašavaju na njihovim internetskim stranicama. Ciljano oglašavanje odnosi se na postavljanje oglasa na temelju demografije i prijašnjih kupovina ili ponašanja kupaca. Za njega je stoga potrebno sustavno praćenje navika i ponašanja ispitanika na internetu.

Primjer: Bolnica i društvo za zdravstveno osiguranje tipični su primjeri voditelja obrade čije se aktivnosti sastoje od opsežne obrade posebnih kategorija osobnih podataka. Podaci koji otkrivaju informacije o zdravlju osoba čine posebne kategorije osobnih podataka prema pravu Vijeća Europe i EU-a te stoga zahtijevaju pojačanu zaštitu. Prema pravu EU-a, genetski i biometrijski podaci također se smatraju posebnim kategorijama. Ako zdravstvene ustanove i osiguravajuća društva obrađuju takve podatke u velikoj mjeri, na temelju OUZP-a dužni su imenovati službenika za zaštitu podataka.

Usto, člankom 37. stavkom 4. OUZP-a utvrđeno je da, s izuzećem triju obveznih slučajeva iz članka 37. stavka 1., u preostalim slučajevima voditelj obrade, izvršitelj obrade ili udruženja i druga tijela koja predstavljaju kategoriju voditelja obrade ili izvršitelja obrade mogu ili – ako to nalaže pravo Unije ili pravo države članice – moraju imenovati službenika za zaštitu podataka.

Druge organizacije nisu zakonski obvezane imenovati SZP-a. Međutim, OUZP-om je utvrđeno da voditelji obrade i izvršitelji obrade mogu dobrovoljno imenovati SZP-a te se istovremeno državama članicama omogućuje da imenovanje službenika proglase obveznim za više vrsta organizacija od onih navedenih u Uredbi⁴⁶⁴.

Kada voditelj obrade imenuje službenika za zaštitu podataka, mora osigurati da je on „na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka” unutar organizacije⁴⁶⁵. Primjerice, SZP-ovi trebaju biti uključeni u savjetovanje o provođenju procjena učinka zaštite podataka te u izradu i vođenje evidencije aktivnosti obrade u organizaciji. Kako bi SZP-ovi učinkovito izvršavali svoje zadatke, voditelji obrade i izvršitelji obrade moraju im osigurati potrebne resurse, uključujući

⁴⁶⁴ Opća uredba o zaštiti podataka, članak 37. stavci 3. i 4.

⁴⁶⁵ *Ibid.*, članak 38. stavak 1.

financijska sredstva, infrastrukturu i opremu. Dodatni zahtjevi uključuju pružanje dovoljno vremena SZP-ovima kako bi ispunili svoje funkcije te redovitu obuku kako bi mogli razvijati svoje stručne vještine i pratiti razvoj zakonodavstva o zaštiti podataka⁴⁶⁶.

OUZP-om se uspostavljaju određena osnovna jamstva kojima se osigurava da službenici za zaštitu podataka neovisno djeluju. Voditelji obrade i izvršitelji obrade moraju osigurati da u provođenju svojih zadataka povezanih sa zaštitom podataka SZP-ovi ne primaju nikakve naputke od društva, kao ni od osoba na najvišim upravljačkim funkcijama. Usto, ne smije ga se razriješiti dužnosti ni kazniti zbog izvršavanja njegovih zadaća⁴⁶⁷. Primjerice, u jednom slučaju SZP savjetuje voditelju ili izvršitelju obrade da provede procjenu učinka zaštite podataka jer smatra da će obrada vjerojatno uzrokovati visok rizik za ispitanike. Društvo se ne slaže sa savjetom SZP-a jer ne smatra da je utemeljen, te stoga odlučuje da neće provesti procjenu učinka. Društvo može zanemariti savjet, ali ne smije službenika razriješiti dužnosti niti ga kazniti jer ga je pružio.

Zadaće i dužnosti SZP-a detaljno su opisane u članku 39. OUZP-a. One uključuju obavezno informiranje i savjetovanje društava i zaposlenika koji obavljaju obradu o njihovim obvezama sukladno zakonodavstvu te praćenje poštovanja propisa EU-a i nacionalnih propisa koji se odnose na zaštitu podataka putem revizija i osposobljavanja osoblja koje sudjeluje u postupcima obrade. SZP-ovi također moraju surađivati s nadzornim tijelom i djelovati kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, kao što je povreda podataka.

Kad je riječ o osobnim podacima kojima rukuju institucije i tijela EU-a, Uredbom (EZ) 45/2001 propisuje se da svaka institucija i tijelo Unije mora imenovati SZP-a. SZP ima obvezu osigurati da se odredbe Uredbe pravilno provode u institucijama i tijelima EU-a te da su i ispitanici i voditelji obrade obaviješteni o svojim pravima i obvezama⁴⁶⁸. Taj je službenik također odgovoran za odgovaranje na zahtjeve Europskog nadzornika za zaštitu podataka (EDPS) i, po potrebi, suradnju s njime. Slično kao i OUZP, Uredba (EZ) 45/2001 sadržava odredbe o neovisnosti SZP-ova u izvršavanju njihovih zadaća te o potrebi za osiguravanjem osoblja i sredstava koji

466 Radna skupina iz članka 29. (2017.), *Smjernice o službenicima za zaštitu podataka („SZP-ovima“)*, WP 243 rev.01, posljednji put revidirane i donesene 5. travnja 2017., točka 3.1.

467 Opća uredba o zaštiti podataka, članak 38. stavci 2. i 3.

468 Vidjeti članak 24. stavak 1. Uredbe (EZ) br. 45/2001 za cjelovit popis zadaća službenika za zaštitu podataka.

su im potrebni⁴⁶⁹. SZP-ove se mora obavijestiti prije nego što neka institucija ili tijelo EU-a (ili odjeli tih organizacija) provede bilo koji postupak obrade te oni moraju voditi evidenciju svih prijavljenih postupaka obrade⁴⁷⁰.

4.3.2. Evidencija aktivnosti obrade

Da bi mogla dokazati sukladnost i preuzeti odgovornost, društva su često zakonski obvezana dokumentirati i evidentirati svoje aktivnosti. Važan su primjer porezni zakoni i revizije, za koje je nužno da sva društva vode opsežnu dokumentaciju i evidenciju. Utvrđivanje sličnih zahtjeva u drugim područjima zakonodavstva, posebice zakonodavstva o zaštiti podataka, također je važno jer je vođenje evidencije važan način za postizanje sukladnosti s propisima o zaštiti podataka. **Pravom EU-a** stoga se propisuje da voditelji obrade ili njihovi predstavnici moraju voditi evidenciju aktivnosti obrade za koje su odgovorni⁴⁷¹. Tom se obavezom nastoji osigurati da nadzorna tijela po potrebi na raspolaganju imaju potrebnu dokumentaciju kako bi potvrdila zakonitost obrade podataka.

Informacije koje se trebaju evidentirati uključuju sljedeće:

- ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka,
- svrhe obrade,
- opis kategorija ispitanika i kategorija osobnih podataka povezanih s obradom,
- informacije o kategorijama primatelja kojima su osobni podaci otkriveni ili će biti otkriveni,
- informacije o tome jesu li ili hoće li osobni podaci biti preneseni u treće zemlje ili međunarodne organizacije,
- ako je to moguće, predviđene rokove za brisanje različitih kategorija osobnih podataka te pregled tehničkih mjera donesenih za osiguravanje sigurnosti obrade⁴⁷².

⁴⁶⁹ Uredba (EZ) br. 45/2001, članak 24. stavci 6. i 7.

⁴⁷⁰ *Ibid.*, članci 25. i 26.

⁴⁷¹ Opća uredba o zaštiti podataka, članak 30.

⁴⁷² *Ibid.*, članak 30. stavak 1.

Obveza vođenja evidencije aktivnosti obrade prema OUZP-u ne odnosi se samo na voditelje obrade nego i na izvršitelje obrade. To je važna novost jer je prije donošenja Uredbe ugovor sklopljen između voditelja i izvršitelja obrade prvenstveno obuhvaćao obveze izvršitelja obrade. Njihova je obveza vođenja evidencije sada izravno predviđena zakonom.

OUZP-om se propisuje i izuzeće od te obveze. Zahtjev vođenja evidencije ne odnosi se na poduzeće ili organizaciju (voditelja ili izvršitelja obrade) s manje od 250 zaposlenika. Međutim, to izuzeće podliježe uvjetima prema kojima dotična organizacija ne smije provoditi obradu koja će vjerojatno dovesti do rizika za prava i slobode ispitanika te prema kojima je obrada samo povremena i ne uključuje posebne kategorije podataka iz članka 9. stavka 1. ni osobne podatke povezane s kaznenim osudama i kažnjivim djelima iz članka 10.

Vođenje evidencije o aktivnostima obrade trebalo bi omogućiti voditeljima obrade i izvršiteljima obrade da dokažu usklađenost s Uredbom. Također bi trebalo omogućiti nadzornim tijelima da prate zakonitost obrade podataka. Ako nadzorno tijelo zatraži pristup toj evidenciji, voditelji obrade i izvršitelji obrade dužni su surađivati i staviti je na raspolaganje.

4.3.3. Procjena učinka zaštite podataka i prethodno savjetovanje

Postupci obrade donose određene rizike za prava pojedinaca. Osobni se podaci mogu izgubiti, otkriti neovlaštenim stranama ili nezakonito obraditi. Rizici se, naravno, razlikuju ovisno o prirodi i opsegu obrade. Primjerice, postupci većih razmjera koji uključuju obradu osjetljivih podataka donose mnogo veći rizik za ispitanike u odnosu na potencijalne rizike kada neko manje društvo obrađuje adrese i osobne telefonske brojeve svojih zaposlenika.

S pojavom novih tehnologija i sve složenijom obradom podataka, voditelji obrade moraju otkloniti takve rizike uz pomoć procjene vjerojatnog učinka predviđene obrade prije početka samog postupka obrade. Time se omogućuje da organizacije pravilno prepoznaju, otklone i umanje rizike unaprijed i tako znatno ograniče vjerojatnost negativnog učinka obrade na pojedince.

Procjene učinka zaštite podataka predviđene su **pravom Vijeća Europe i EU-a**. Unutar pravnog okvira Vijeća Europe, člankom 10. stavkom 2. modernizirane Konvencije br. 108, od ugovornih strana zahtijeva se da osiguraju da voditelji obrade i izvršitelji

obrade „ispitaju vjerojatni učinak planirane obrade podataka na prava i temeljne slobode ispitanika prije početka takve obrade” te da na temelju te procjene osmisle obradu tako da se spriječe ili umanje rizici povezani s njome.

Pravom EU-a nameće se slična, ali detaljnija obveza voditeljima obrade koji su obuhvaćeni područjem primjene OUZP-a. Člankom 35. utvrđuje se da se procjena učinka mora provesti kada je vjerojatno da će obrada prouzročiti visok rizik za prava i slobode pojedinaca. U Uredbi nije utvrđeno kako se vjerojatnost rizika treba procijeniti, nego se samo navodi koji su rizici mogući⁴⁷³. Naveden je popis postupaka obrade koji se smatraju visokorizičnima i za koje je prethodna procjena učinka posebno važna. To su prvenstveno sljedeći slučajevi:

- osobni podaci obrađuju se radi donošenja odluka o pojedincima na temelju bilo kakve sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima (izrada profila),
- osjetljivi podaci ili osobni podaci u vezi s kaznenim osudama i kažnjivim djelima obrađuju se u većoj mjeri,
- obrada uključuje opsežno, sustavno praćenje javno dostupnih područja.

Nadzorna tijela moraju donijeti i javno objaviti popis vrsta postupaka obrade koji podliježu procjenama učinka. Također mogu uspostaviti popis postupaka obrade koji su izuzeti iz te obveze⁴⁷⁴.

Kada je potrebna procjena učinka, voditelji obrade moraju procijeniti nužnost i proporcionalnost obrade te moguće rizike za prava pojedinaca. Procjena učinka također mora uključivati planirane mjere sigurnosti za otklanjanje utvrđenih rizika. Za uspostavljanje popisa nadzorna tijela država članica moraju surađivati međusobno i s Europskim odborom za zaštitu podataka. Time će se osigurati dosljedan pristup na razini EU-a za postupke u kojima je potrebna procjena učinka, a voditeljima obrade bit će postavljeni slični zahtjevi neovisno o njihovoj lokaciji.

⁴⁷³ *Ibid.*, preambula, uvodna izjava 75.

⁴⁷⁴ *Ibid.*, članak 35. stavci 4. i 5.

Ako se nakon procjene učinka čini da će obrada dovesti do visokog rizika za prava pojedinaca, a nisu uvedene mjere za umanjivanje tog rizika, voditelj obrade mora se savjetovati s nadležnim nadzornim tijelom prije početka postupka obrade⁴⁷⁵.

Radna skupina iz članka 29. izdala je smjernice o procjeni učinka zaštite podataka te o tome kako utvrditi vjerojatnost da će obrada dovesti do visokog rizika⁴⁷⁶. Skupina je razvila devet kriterija za utvrđivanje nužnosti procjene učinka zaštite podataka u pojedinom slučaju⁴⁷⁷: 1) procjena ili bodovanje; 2) automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom; 3) sustavno praćenje; 4) osjetljivi podaci; 5) opsežna obrada podataka; 6) podudarajući ili kombinirani skupovi podataka; 7) podaci koji se odnose na osjetljive ispitanike; 8) inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja; 9) situacija u kojoj sama obrada „sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora“. Radna skupina iz članka 29. uvela je korisno pravilo prema kojemu postupci obrade koji ispunjavaju manje od dvaju kriterija predstavljaju niži rizik i ne zahtijevaju procjenu zaštite podataka, dok postupci koji ispunjavaju dva ili više kriterija zahtijevaju procjenu. Ako nije jasno je li procjena učinka zaštite podataka potrebna, Radna skupina iz članka 29. preporučuje da se ona ipak provede jer „voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka“⁴⁷⁸. Važno je provesti procjenu učinka zaštite podataka pri uvođenju nove tehnologije za obradu podataka⁴⁷⁹.

4.3.4. Kodeksi ponašanja

Kodeksi ponašanja namijenjeni su uporabi u nekoliko industrijskih sektora kako bi se opisala i utvrdila primjena OUZP-a u pojedinim sektorima. Voditeljima obrade i izvršiteljima obrade osobnih podataka izrada kodeksa može pomoći da znatno poboljšaju provedbu propisa o zaštiti podataka EU-a i usklađenost s njima. Stručno znanje članova sektora pomoći će u pronalasku praktičnih rješenja za koje je izgledno da će biti prihvaćena. Potvrđujući važnost takvih kodeksa u učinkovitoj provedbi zakonodavstva o zaštiti podataka, OUZP-om se države članice, nadzorna tijela, Komisija

475 *Ibid.*, članak 36. stavak 1.; Radna skupina iz članka 29. (2017.), *Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik“ u smislu Uredbe 2016/679*, WP 248 rev.01, Bruxelles, 4. listopada 2017.

476 Radna skupina iz članka 29. (2017.), *Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik“ u smislu Uredbe 2016/679*, WP 248 rev.01, Bruxelles, 4. listopada 2017.

477 *Ibid.*, str. 9.–11.

478 *Ibid.*, str. 9.

479 *Ibid.*

i Europski odbor za zaštitu podataka pozivaju da potaknu izradu kodeksa ponašanja koji su namijenjeni promicanju pravilne provedbe Uredbe na razini EU-a⁴⁸⁰. Kodeksima se može utvrditi provedba Uredbe u pojedinim sektorima, uključujući pitanja poput prikupljanja osobnih podataka, informacija koje se trebaju pružiti ispitanicima i javnosti te ostvarivanja prava ispitanika.

Kako bi se osiguralo da su kodeksi ponašanja usklađeni s odredbama OUZP-a, oni se moraju podnijeti nadležnom nadzornom tijelu prije donošenja. Nadzorno tijelo daje mišljenje o tome je li nacrt kodeksa u skladu s Uredbom te takav nacrt kodeksa odobrava ako smatra da osigurava dovoljno prikladne zaštitne mjere⁴⁸¹. Nadzorna tijela moraju objaviti odobrene kodekse ponašanja, kao i kriterije na kojima se odobrenje temelji. Ako se nacrt kodeksa ponašanja odnosi na aktivnosti obrade u nekoliko država članica, nadležno nadzorno tijelo prije davanja odobrenja podnosi nacrt kodeksa, izmjenu ili proširenje Europskom odboru za zaštitu podataka, koji daje mišljenje o usklađenosti kodeksa s OUZP-om. Komisija može provedbenim aktima odlučiti da odobreni kodeks ponašanja koji joj je predan ima opću valjanost unutar Unije.

Pridržavanjem kodeksa ponašanja ostvaruju se važne prednosti kako za ispitanike tako i za voditelje obrade i izvršitelje obrade. Takvi kodeksi pružaju detaljne smjernice kojima se pravni zahtjevi mogu prilagoditi pojedinim sektorima te kojima se potiče transparentnost aktivnosti obrade podataka. Voditelji obrade i izvršitelji obrade također mogu iskoristiti pridržavanje kodeksa kao jasan dokaz svoje usklađenosti s pravom EU-a i kao način poboljšanja svog javnog ugleda kao organizacije koje su predane zaštiti podataka u svojem radu i stavljaju je na prvo mjesto. Odobreni kodeksi ponašanja u kombinaciji s obvezujućim i provedivim obvezama mogu se upotrijebiti kao odgovarajuće zaštitne mjere za prijenos podataka u treće zemlje. Da bi se osiguralo da su organizacije koje se pridržavaju kodeksa ponašanja doista i sukladne s njima, može se imenovati posebno tijelo (koje akreditira nadležno nadzorno tijelo) radi praćenja i osiguravanja sukladnosti. Za učinkovito ispunjavanje svojih zadaća to tijelo mora biti neovisno, imati dokazanu stručnost u pitanjima koja su uređena kodeksom ponašanja te imati transparentne postupke i strukture za rješavanje pritužbi na kršenje kodeksa⁴⁸².

⁴⁸⁰ Opća uredba o zaštiti podataka, članak 40. stavak 1.

⁴⁸¹ *Ibid.*, članak 40. stavak 5.

⁴⁸² *Ibid.*, članak 41. stavci 1. i 2.

Prema **pravu Vijeća Europe**, moderniziranom Konvencijom br. 108 utvrđeno je da se razina zaštite podataka koja je zajamčena nacionalnim zakonodavstvom može korisno pojačati dobrovoljnim regulatornim mjerama, poput kodeksa dobre prakse ili kodeksa profesionalnog ponašanja. Međutim, to su isključivo dobrovoljne mjere prema moderniziranoj Konvenciji br. 108; nije moguće uspostaviti nikakvu pravnu obvezu za uvođenje takvih mjera, iako se to preporučuje, te takve mjere same po sebi nisu dovoljne da bi se osigurala potpuna usklađenost s Konvencijom⁴⁸³.

4.3.5. Certificiranje

Uz kodekse ponašanja, mehanizmi certificiranja te pečati i oznake zaštite podataka dodatno su sredstvo s pomoću kojega voditelji obrade i izvršitelji obrade mogu dokazati svoju sukladnost s OUZP-om. U tu se svrhu Uredbom propisuje dobrovoljan sustav certificiranja putem kojega određena tijela ili nadzorna tijela mogu izdavati certifikate. Voditelji obrade i izvršitelji obrade koji odluče upotrebljavati mehanizam certificiranja mogu ostvariti veću vidljivosti i vjerodostojnost s obzirom na to da certifikati, pečati i oznake omogućuju ispitanicima da brzo procijene razinu zaštite pri obradi podataka pojedinih organizacija. Važno je napomenuti da činjenica da neki voditelj ili izvršitelj obrade posjeduje certifikat ne podrazumijeva da su njegove dužnosti i odgovornosti nužno u skladu sa svim odredbama Uredbe.

4.4. Tehnička i integrirana zaštita podataka

Tehnička zaštita podataka

Pravom EU-a od voditelja obrade zahtijeva se uspostavljanje mjera za učinkovitu primjenu načela zaštite podataka i uključenje potrebnih zaštitnih mjera u obradu radi ispunjavanja zahtjeva iz Uredbe i zaštite prava ispitanika⁴⁸⁴. Te se mjere trebaju provoditi i u trenutku obrade i prilikom utvrđivanja sredstva obrade. Prilikom provedbe tih mjera voditelj obrade mora uzeti u obzir najnovija dostignuća, troškove provedbe, prirodu, opseg i svrhe obrade osobnih podataka te rizike za prava i slobode ispitanika i ozbiljnost tih rizika⁴⁸⁵.

483 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 33.

484 Opća uredba o zaštiti podataka, članak 25. stavak 1.

485 Vidjeti: Radna skupina iz članka 29. (2017.), *Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik” u smislu Uredbe 2016/679, WP 248 rev.01*, 4. listopada 2017. Vidjeti i ENISA (2015.), *Privacy and Data Protection by Design-from policy to engineering* (Privatnost i tehnička zaštita podataka: od politike do projektiranja), 12. siječnja 2015.

Prema pravu Vijeća Europe, od voditelja obrade i izvršitelja obrade zahtijeva se da procijene vjerojatan učinak obrade osobnih podataka na prava i slobode ispitanika prije početka same obrade. Usto, voditelji obrade i izvršitelji obrade dužni su organizirati obradu podataka tako da se spriječi ili umanjuje rizik od miješanja u ta prava i slobode te provesti tehničke i organizacijske mjere koje su osmišljene uzimajući u obzir aspekt prava na zaštitu osobnih podataka u svim fazama obrade podataka⁴⁸⁶.

Integrirana zaštita podataka

Prema pravu EU-a, od voditelja obrade zahtijeva se da provede odgovarajuće mjere kako bi osigurao da se integriranim načinom obrađuju samo osobni podaci koji su nužni za određenu svrhu. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost⁴⁸⁷. Takvom se mjerom mora osigurati, primjerice, da nemaju svi zaposlenici voditelja obrade pristup osobnim podacima osoba čiji se podaci obrađuju. Dodatne je smjernice razvio EDPS u *Paketu alata za određivanje nužnosti mjera*⁴⁸⁸.

Prema pravu Vijeća Europe od voditelja obrade i izvršitelja obrade zahtijeva se da provedu tehničke i organizacijske mjere kako bi u obzir uzeli aspekt prava na zaštitu podataka te da provedu tehničke i organizacijske mjere koje su osmišljene uzimajući u obzir aspekt prava na zaštitu podataka u svim fazama obrade podataka⁴⁸⁹.

ENISA je 2016. objavila izvješće o dostupnim alatima i uslugama za privatnost⁴⁹⁰. Među ostalim, ta procjena uključuje kazalo kriterija i parametara koji predstavljaju pokazatelje dobrih odnosno loših praksi u vezi s privatnošću. Neki su kriteriji izravno povezani s odredbama OUZP-a, poput upotrebe pseudonimizacije i odobrenih mehanizama certificiranja, a drugima se pružaju inovativne inicijative za osiguravanje tehničke i integrirane privatnosti. Primjerice, kriterij upotrebljivosti može poslužiti za poboljšanje privatnosti iako nije izravno s njome povezan jer može omogućiti šire usvajanje alata ili usluge za privatnost. Šira javnost može u manjoj mjeri usvajati

486 Modernizirana Konvencija br. 108, članak 10. stavci 2. i 3., Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 89.

487 Opća uredba o zaštiti podataka, članak 25. stavak 2.

488 Europski nadzornik za zaštitu podataka (EDPS) (2017.), *Necessity Toolkit* (Paket alata za određivanje nužnosti mjera), Bruxelles, 11. travnja 2017.

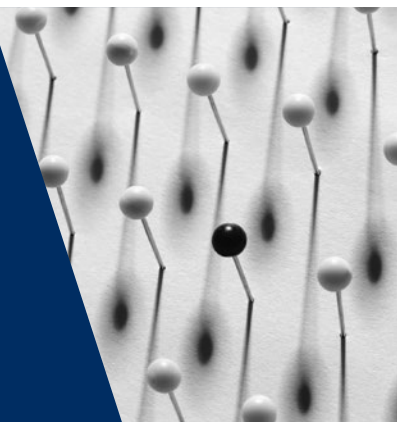
489 Modernizirana Konvencija br. 108, članak 10. stavak 3., Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 89.

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools* (Kontrolna matrica PET-ova: sustavni pristup za ocjenjivanje alata za privatnost na mreži i u mobilnoj telefoniji), 20. prosinca 2016.

alate za privatnost koje je teže provesti u praksi, čak i ako pružaju snažnu zaštitu privatnosti. Usto, kriterij razvijenosti i stabilnosti alata za privatnost, odnosno način na koji se alat razvija s vremenom i prilagođava postojećim ili novim izazovima u vezi s privatnošću, od ključne je važnosti. Druge tehnologije pojačane privatnosti, primjerice u kontekstu sigurnih komunikacija, uključuju šifriranje „s kraja na kraj” (komunikaciju u kojoj isključivo osobe koje komuniciraju mogu čitati poruke); šifriranje klijent–poslužitelj (šifriranje komunikacijskog kanala koji se uspostavlja između klijenta i poslužitelja); autentifikaciju (provjeru identiteta strana koje komuniciraju) te anonimnu komunikaciju (nijedna treća strana ne može identificirati strane koje komuniciraju).

5

Neovisni nadzor



EU	Obuhvaćena pitanja	Vijeće Europe
Povelja (dostupna na engleskom jeziku), članak 8. stavak 3. Ugovor o funkcioniranju Europske unije (dostupan na engleskom jeziku), članak 16. stavak 2. Opća uredba o zaštiti podataka, članci od 51. do 59. SEU, C-518/07, <i>Europska komisija protiv Savezne Republike Njemačke</i> [VV], 2010. SEU, C-614/10, <i>Europska komisija protiv Republike Austrije</i> [VV], 2012. SEU, C-288/12, <i>Europska komisija protiv Mađarske</i> [VV], 2014. SEU, C-362/14, <i>Maximillian Schrems protiv Data Protection Commissioner</i> [VV], 2015.	Nadzorna tijela	Modernizirana Konvencija br. 108, članak 15.
Opća uredba o zaštiti podataka, članci od 60. do 67.	Suradnja nadzornih tijela	Modernizirana Konvencija br. 108, članci od 16. do 21.
Opća uredba o zaštiti podataka, članci od 68. do 76.	Europski odbor za zaštitu podataka	

Ključne točke

- Neovisni nadzor ključni je element europskog zakonodavstva o zaštiti podataka i utvrđen je člankom 8. stavkom 3. Povelje.
- Radi osiguravanja učinkovite zaštite podataka, nacionalnim zakonodavstvom moraju biti uspostavljena neovisna nadzorna tijela.
- Nadzorna tijela moraju djelovati potpuno neovisno, a neovisnost im se mora zajamčiti pravom na temelju kojeg su uspostavljena i mora se odražavati u posebnoj organizacijskoj strukturi nadzornog tijela.
- Nadzorna tijela imaju posebne ovlasti i zadaće. One, među ostalim, uključuju sljedeće:
 - nadzor i promicanje zaštite podataka na nacionalnoj razini,
 - savjetovanje ispitanika i voditelja obrade, kao i vlade i šire javnosti,
 - saslušanje prigovora i pomaganje ispitanicima u vezi s navodnim kršenjem prava na zaštitu podataka,
 - nadzor voditelja obrade i izvršitelja obrade.
- Nadzorna tijela također imaju ovlast intervenirati po potrebi, i to:
 - upozoravanjem, opominjanjem ili čak novčanim kažnjavanjem voditelja obrade i izvršitelja obrade,
 - izdavanjem naloga da se podaci isprave, blokiraju ili izbrišu,
 - nametanjem zabrane obrade ili upravne novčane kazne,
 - upućivanjem slučajeva sudu.
- Budući da obrada osobnih podataka često uključuje voditelje obrade i izvršitelje obrade te ispitanike koji se nalaze u različitim državama, nadzorna tijela moraju međusobno surađivati na prekograničnim pitanjima kako bi osigurala učinkovitu zaštitu pojedinaca u Europi.
- Općom uredbom o zaštiti podataka u EU-u se uspostavlja jedinstveni mehanizam za slučajeve prekogranične obrade. Neka društva obavljaju prekogranične aktivnosti obrade zbog obrade osobnih podataka u kontekstu aktivnosti poslovnih nastana u više od jedne države članice ili u kontekstu jedinog poslovnog nastana u Uniji, koji bitno utječe na ispitanike u više od jedne države članice. Sukladno mehanizmu, takva društva moraju surađivati samo s jednim nacionalnim nadzornim tijelom za zaštitu podataka.

- Mehanizam suradnje i konzistentnosti omogućit će koordinirani pristup svih nadzornih tijela koja sudjeluju u slučaju. Vodeće nadzorno tijelo glavnog ili jedinog poslovnog nastana savjetovat će se s drugim nadležnim nadzornim tijelima i podnijeti im svoj nacrt odluke.
- Slično kao i trenutna Radna skupina iz članka 29., nadzorno tijelo svake države članice i Europski nadzornik za zaštitu podataka (EDPS) bit će članovi Europskog odbora za zaštitu podataka.
- Zadaće Europskog odbora za zaštitu podataka uključuju, primjerice, praćenje pravilne provedbe Uredbe, savjetovanje Komisije o relevantnim pitanjima te izdavanje mišljenja, smjernica ili najboljih praksi o različitim temama.
- Osnovna je razlika da Europski odbor za zaštitu podataka neće samo izdavati mišljenja na temelju Direktive 95/46/EZ. Također će donositi obvezujuće odluke o slučajevima u kojima nadzorno tijelo podnese relevantan i obrazložen prigovor na jedinstvene kontaktne točke, kada postoje oprečna stajališta o tome koje je nadzorno tijelo vodeće te, naposljetku, kada nadležno nadzorno tijelo ne zatraži ili ne uzme u obzir mišljenje Odbora. Cilj je osigurati dosljednu provedbu Uredbe u svim državama članicama.

Neovisni nadzor ključni je element europskog zakonodavstva o zaštiti podataka. I prema pravu EU-a i pravu Vijeća Europe postojanje neovisnih nadzornih tijela smatra se neophodnim za učinkovitu zaštitu prava i sloboda pojedinaca u pogledu obrade njihovih osobnih podataka. Budući da je danas obrada podataka sveprisutna i sve složenija pa je teško razumljiva prosječnoj osobi, ta su tijela čuvari digitalnog doba. Postojanje neovisnih nadzornih tijela u EU-u smatra se jednim od temeljnih elemenata prava na zaštitu osobnih podataka i zaštićen je primarnim pravom Unije. Člankom 8. stavkom 3. Povelje Europske unije o temeljnim pravima te člankom 16. stavkom 2. UFEU-a zaštita osobnih podataka prepoznaje se kao temeljno pravo i potvrđuje se da sukladnost s propisima o zaštiti podataka podliježe kontroli neovisnog tijela.

Važnost neovisnog nadzora za zakonodavstvo o zaštiti podataka potvrđena je i sudskom praksom.

Primjer: U predmetu *Schrems*⁴⁹¹ SEU je razmatrao je li prosljeđivanje osobnih podataka u Sjedinjene Američke Države (SAD) u sklopu prvog Sporazuma o sigurnoj luci između EU-a i SAD-a u skladu sa zakonodavstvom EU-a o zaštiti podataka u kontekstu otkrića Edwarda Snowdena o masovnom nadzoru Nacionalne sigurnosne agencije (NSA) SAD-a. Prijenos osobnih podataka u SAD

⁴⁹¹ SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VV], 6. listopada 2015.

temeljio se na odluci Europske komisije donesenoj 2000., prema kojoj je dopušten prijenos osobnih podataka iz organizacija u EU-u organizacijama u SAD-u koje vrše vlastito potvrđivanje u sklopu sustava sigurne luke, na temelju toga da se sustavom osigurava odgovarajuća razina zaštite osobnih podataka. Kada je primilo zahtjev za ispitivanje pritužbe podnositelja zahtjeva koja se odnosila na zakonitost prijenosa podataka nakon Snowdenovih otkrića, irsko nadzorno tijelo odbilo je pritužbu, uz obrazloženje da Odluka Komisije o primjerenosti režima zaštite podataka SAD-a, koji se odražava u načelima „sigurne luke” („Odluka o sigurnoj luci”), sprečava daljnje ispitivanje pritužbe.

Međutim, SEU je smatrao da postojanje odluke Komisije koja omogućuje prijenos podataka u treće zemlje koje osiguravaju odgovarajuće razine zaštite ne podrazumijeva ukidanje ni smanjivanje ovlasti nacionalnih nadzornih tijela. SEU je istaknuo kako ovlasti tih tijela u području praćenja i osiguranja sukladnosti s propisima EU-a o zaštiti podataka proizlaze iz primarnog prava EU-a, točnije članka 8. stavka 3. Povelje i članka 16. stavka 2. UFEU-a. „Stoga je uspostava neovisnih nadzornih nacionalnih tijela [...] osnovni dio poštovanja zaštite pojedinaca u vezi s obradom osobnih podataka.”⁴⁹²

SEU je stoga odlučio da čak i kada je prijenos osobnih podataka podvrgnut Komisijinoj odluci o primjerenosti, ako je pritužba podnesena nacionalnom nadzornom tijelu, to tijelo mora ispitati pritužbu s dužnom pažnjom. Nadzorno tijelo može odbiti pritužbu ako zaključi da je neutemeljena. U tom slučaju, SEU je istaknuo da pravo na djelotvoran pravni lijek pred sudom podrazumijeva da pojedinci moraju imati mogućnost pobijanja takve odluke pred nacionalnim sudovima, koji mogu predmet proslijediti SEU-u radi prethodne odluke o valjanosti Komisijine odluke. Kada nadzorno tijelo smatra da je pritužba utemeljena, mora moći sudjelovati u sudskom postupku i iznijeti predmet pred nacionalnim sudovima. Nacionalni sudovi mogu uputiti predmet SEU-u jer je to jedino tijelo koje ima ovlast za odlučivanje o valjanosti Komisijine odluke o primjerenosti⁴⁹³.

SEU je zatim preispitao valjanost Odluke o sigurnoj luci kako bi utvrdio je li sustav prijenosa u skladu s propisima EU-a o zaštiti podataka. Zaključio je da se člankom 3. Odluke o sigurnoj luci ograničavaju ovlasti nacionalnih

492 SEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [WV], 6. listopada 2015., t. 41.

493 *Ibid.*, t. od 53. do 66.

nadzornih tijela (koje su im dodijeljene Direktivom o zaštiti podataka) da poduzmu mjere za sprečavanje prijenosa podataka u slučaju neodgovarajuće razine zaštite osobnih podataka u SAD-u. S obzirom na važnost neovisnih nadzornih tijela za osiguranje sukladnosti sa zakonodavstvom o zaštiti podataka, SEU je smatrao da na temelju Direktive o zaštiti podataka i Povelje Komisija nije ovlaštena za ograničavanje ovlasti neovisnim nadzornim tijelima na taj način. Ograničenje ovlasti nadzornih tijela bilo je jedan od razloga zbog kojih je SEU Odluku o sigurnoj luci proglasio nevaljanom.

Europskim pravom stoga se zahtijeva neovisan nadzor kao važan mehanizam za osiguranje učinkovite zaštite podataka. Neovisna nadzorna tijela prva su točka kontakta za ispitanike u slučajevima povreda podataka⁴⁹⁴. Unutar prava Unije i Vijeća Europe obavezno je uspostavljanje nadzornih tijela. U obama pravnim okvirima opisuju se zadaće i ovlasti tih tijela na sličan način kao i u OUZP-u. Stoga bi nadzorna tijela u načelu trebala funkcionirati na jednak način unutar prava EU-a i Vijeća Europe⁴⁹⁵.

5.1. Neovisnost

Pravom EU-a i Vijeća Europe propisuje se da svako nadzorno tijelo djeluje potpuno neovisno pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti⁴⁹⁶. Neovisnost nadzornog tijela i njegovih članova, kao i osoblja, od izravnih ili neizravnih vanjskih utjecaja ključno je za osiguranje potpune objektivnosti pri donošenju odluka o pitanjima zaštite podataka. Osim što zakonodavstvo na kojem se temelji osnivanje nadzornog tijela mora sadržavati odredbe koje izričito jamče neovisnost, i sama organizacijska struktura tijela mora biti dokaz njegove neovisnosti. SEU je 2010. prvi put razmatrao mjeru u kojoj nadzorna tijela za zaštitu podataka moraju biti neovisna⁴⁹⁷. Navedeni primjeri ilustriraju definiciju SEU-a o značenju „potpune neovisnosti”.

⁴⁹⁴ Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (d).

⁴⁹⁵ *Ibid.*, članak 51.; modernizirana Konvencija br. 108, članak 15.

⁴⁹⁶ Opća uredba o zaštiti podataka, članak 52. stavak 1.; modernizirana Konvencija br. 108, članak 15. stavak 5.

⁴⁹⁷ FRA (2010.), *Fundamental rights: challenges and achievements in 2010* (Temeljna prava: izazovi i postignuća u 2010.), godišnje izvješće za 2010., str. 59.; FRA (2010.), *Data Protection in the European Union: the role of National Data Protection Authorities* (Zaštita podataka u Europskoj uniji: uloga nacionalnih tijela za zaštitu podataka), svibanj 2010.

Primjer: U predmetu *Europska komisija protiv Savezne Republike Njemačke*⁴⁹⁸ Europska komisija zatražila je od SEU-a izjavu da je Njemačka netočno prenijela zahtjev „potpune neovisnosti” nadzornih tijela odgovornih za osiguravanje zaštite podataka i na taj način nije ispunila svoje obveze iz članka 28. stavka 1. Direktive o zaštiti podataka. Prema mišljenju Komisije, Njemačka je prekršila zahtjev neovisnosti time što je pod nadzor države stavila tijela odgovorna za nadzor obrade osobnih podataka u različitim saveznm državama (*Länder*) kako bi osigurala sukladnost sa zakonodavstvom o zaštiti podataka.

SEU je istaknuo da se riječi „potpuno neovisno” moraju tumačiti na temelju stvarnog teksta te odredbe i na temelju ciljeva i sustava zakonodavstva EU-a o zaštiti podataka⁴⁹⁹. SEU je naglasio da su nadzorna tijela „čuvari” prava povezanih s obradom osobnih podataka. Stoga se smatra da je njihova uspostava u državama članicama „osnovni dio poštovanja zaštite pojedinaca u vezi s obradom osobnih podataka”⁵⁰⁰. SEU je zaključio da „u izvršavanju svojih obveza nadzorna tijela moraju postupati objektivno i nepristrano. Zbog toga moraju biti lišena svih vanjskih utjecaja, uključujući izravan ili neizravan utjecaj javnih tijela”⁵⁰¹.

SEU je također utvrdio da značenje „potpune neovisnosti” treba tumačiti u svjetlu neovisnosti EDPS-a kako je definirana u Uredbi o zaštiti podataka u institucijama Europske unije. U toj Uredbi konceptom neovisnosti podrazumijeva se da EDPS ne smije niti tražiti niti prihvaćati naputke drugih.

U skladu s tim, SEU je smatrao da njemačka nadzorna tijela nisu bila potpuno neovisna u smislu zakonodavstva EU-a o zaštiti podataka jer su ih nadzirala javna tijela.

Primjer: U predmetu *Europska komisija protiv Republike Austrije*⁵⁰² SEU je naglasio slične probleme u vezi s neovisnošću određenih članova i osoblja austrijskog tijela za zaštitu podataka (Komisija za zaštitu podataka, DSK). SEU je zaključio da je Savezni kancelar prekršio zahtjev neovisnosti utvrđen u zakonodavstvu EU-a o zaštiti podataka jer je osigurao radnu snagu

498 SEU, C-518/07, *Europska komisija protiv Savezne Republike Njemačke* [VV], 9. ožujka 2010, t. 27.

499 *Ibid.*, t. 17. i 29.

500 *Ibid.*, t. 23.

501 *Ibid.*, t. 25.

502 SEU, C-614/10, *Europska komisija protiv Republike Austrije* [VV], 16. listopada 2012., t. 59. i 63.

nadzornog tijela. SEU je također smatrao da se zahtjevom za informiranje Kancelara o njegovu radu u svakom trenutku poništava potpuna neovisnost nadzornog tijela.

Primjer: U predmetu *Europska komisija protiv Mađarske*⁵⁰³ zabranjene su slične nacionalne prakse koje su utjecale na neovisnost radne snage. SEU je istaknuo da treba ispitati podrazumijeva li „zahtjev [...] da svako nadzorno tijelo izvršava funkcije koje su mu povjerene potpuno neovisno, obvezu za državu članicu o kojoj se radi da poštuje trajanje mandata takvog nacionalnog tijela do isteka roka koji je prvotno predviđen”. SEU je također smatrao da je „okončavši prijevremeno mandat neovisnog nadzornog tijela za zaštitu osobnih podataka, Mađarska povrijedila obveze koje ima na temelju Direktive 95/46/EZ [...]”.

Pojam i kriteriji „potpune neovisnosti” sada su izričito utvrđeni u OUZP-u, koji sadržava načela uspostavljena presudama SEU-a. Sukladno Uredbi, potpuna neovisnost pri obavljanju zadaća ili izvršavanju ovlasti podrazumijeva sljedeće⁵⁰⁴:

- članovi svakog nadzornog tijela moraju biti slobodni od vanjskog utjecaja, bilo izravnog bilo neizravnog, te ne smiju tražiti niti primati upute ni od koga,
- članovi svakog nadzornog tijela moraju se suzdržavati od svih radnji koje nisu u skladu s njihovim dužnostima kako bi se spriječio sukob interesa,
- države članice moraju osigurati da svako nadzorno tijelo ima ljudske, tehničke i financijske resurse te infrastrukturu potrebnu za djelotvorno obavljanje svojih zadaća,
- države članice moraju osigurati da svako nadzorno tijelo odabire vlastito osoblje,
- financijska kontrola kojoj svako nadzorno tijelo podliježe sukladno nacionalnom zakonodavstvu ne smije utjecati na njegovu neovisnost. Nadzorna tijela moraju imati zasebne, javne godišnje proračune koji im omogućuju pravilan rad.

503 SEU, C-288/12, *Europska komisija protiv Mađarske* [VV], 8. travnja 2014., t. 50. i 67.

504 Opća uredba o zaštiti podataka, članak 52.

Neovisnost nadzornih tijela smatra se ključnim zahtjevom i na temelju prava Vijeća Europe. Moderniziranom Konvencijom br. 108 utvrđuje se da bi svako nadzorno tijelo „pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti trebalo djelovati potpuno neovisno i nepristrano“, bez traženja ili prihvaćanja naputaka⁵⁰⁵. Na taj se način Konvencijom potvrđuje da ta tijela ne mogu učinkovito štiti prava i slobode pojedinaca u vezi s obradom podataka ako ne mogu vršiti svoje funkcije potpuno neovisno. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 utvrđuje se niz elemenata koji doprinose zaštiti te neovisnosti. Ti elementi uključuju mogućnost da nadzorna tijela zapošljavaju svoje osoblje i donose odluke bez vanjskog utjecaja, kao i čimbenike povezane s trajanjem njihovih funkcija i uvjetima u kojima mogu prestati vršiti te funkcije⁵⁰⁶.

5.2. Nadležnost i ovlasti

Prema pravu EU-a, u OUZP-u se navode nadležnosti i organizacijska struktura nadzornih tijela te se propisuje da ona moraju biti nadležna i imati ovlast za izvršavanje zadaća utvrđenih u Uredbi.

Nadzorno tijelo glavno je tijelo u sklopu nacionalnog zakonodavstva koje osigurava usklađenost sa zakonodavstvom EU-a o zaštiti podataka. Osim praćenja, nadzorna tijela imaju širok spektar zadaća i ovlasti koje uključuju proaktivne i preventivne aktivnosti nadzora. Kako bi izvršavala te zadaće, nadzorna tijela moraju imati odgovarajuće istražne, korektivne i savjetodavne ovlasti utvrđene u člancima 57. i 58. OUZP-a, kao što su⁵⁰⁷:

- savjetovanje voditelja obrade i ispitanika o svim aspektima zaštite podataka,
- odobravanje standardnih ugovornih klauzula, obvezujućih korporativnih pravila ili administrativnih dogovora,
- istraživanje postupaka obrade i poduzimanje mjera sukladno tome,
- zahtijevanje svih informacija koje su važne za nadzor aktivnosti voditelja obrade,

⁵⁰⁵ Modernizirana Konvencija br. 108, članak 15. stavak 5.

⁵⁰⁶ Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108.

⁵⁰⁷ Opća uredba o zaštiti podataka, članci 57. i 58. Vidjeti i Konvenciju br. 108, Dodatni protokol, članak 1.

- izdavanje upozorenja ili službenih opomena voditeljima obrade te naređivanje voditeljima obrade da ispitanike obavijeste o povredama osobnih podataka,
- naređivanje ispravljanja, blokiranja, brisanja ili uništenja podataka,
- nametanje privremene ili konačne zabrane obrade ili izricanje upravne novčane kazne,
- upućivanje predmeta sudu.

Kako bi moglo izvršavati svoje funkcije, nadzorno tijelo mora imati pristup svim osobnim podacima i informacijama nužnim za istragu, kao i pristup svim prostorijama u kojima voditelj obrade čuva odgovarajuće informacije. Prema SEU-u, ovlasti nadležnog tijela moraju se široko tumačiti kako bi se osigurala potpuna učinkovitost zaštite podataka za ispitanike u EU-u.

Primjer: U predmetu *Schrems* SEU je razmatrao je li prijenos osobnih podataka u SAD u sklopu prvog Sporazuma o sigurnoj luci između EU-a i SAD-a u skladu sa zakonodavstvom EU-a o zaštiti podataka u kontekstu otkrića Edwarda Snowdena. SEU je zaključio da nacionalna nadzorna tijela koja djeluju u svojstvu neovisnih voditelja obrade podataka koju vrše voditelji obrade mogu spriječiti prijenos osobnih podataka u treću zemlju unatoč odluci o primjerenosti ako postoje utemeljeni dokazi da u toj trećoj zemlji više nije zajamčena odgovarajuća zaštita⁵⁰⁸.

Svako nadzorno tijelo nadležno je za izvršavanje istražnih ovlasti i ovlasti intervencije unutar svojeg državnog područja. Međutim, budući da su aktivnosti voditelja obrade i izvršitelja obrade često prekogranične te obrada podataka utječe na ispitanike u više država članica, postavlja se pitanje o raspodjeli nadležnosti na različita nadzorna tijela. SEU je imao priliku razmotriti to pitanje u predmetu *Weltimmo*.

Primjer: U predmetu *Weltimmo*⁵⁰⁹ SEU je razmatrao nadležnost nacionalnih nadzornih tijela u pitanjima koja se odnose na organizacije koje nemaju poslovni nastan unutar njegove sudske nadležnosti. *Weltimmo* je bilo društvo

⁵⁰⁸ SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VJ], 6. listopada 2015., t. od 26. do 36. i od 40. do 41.

⁵⁰⁹ SEU, C-230/14, *Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. listopada 2015.

s registriranim sjedištem u Slovačkoj koje je upravljalo internetskom stranicom za posredovanje nekretninama u Mađarskoj. Oglašivači su podnijeli pritužbu mađarskom nadzornom tijelu za zaštitu podataka zbog kršenja mađarskog zakona o zaštiti podataka, a to je tijelo nametnulo novčanu kaznu društvu Weltimmo. Društvo je osporilo novčanu kaznu pred nacionalnim sudovima te je predmet proslijeđen SEU-u kako bi utvrdio dopušta li Direktiva EU-a o zaštiti podataka nadzornim tijelima određene države članice da primijeni vlastite nacionalne zakone o zaštiti podataka na društvo s registriranim sjedištem u drugoj državi članici.

SEU je protumačio članak 4. stavak 1. točku (a) Direktive o zaštiti podataka na način da se njime dopušta primjena zakona o zaštiti podataka određene države članice koja nije država članica u kojoj voditelj obrade ima registrirano sjedište „ako on putem stabilnih aranžmana na području te države članice obavlja, čak i najmanju, efektivnu i stvarnu djelatnost u okviru koje se ta obrada provodi”. SEU je istaknuo da je, na temelju informacija koje su mu iznesene, društvo Weltimmo obavljalo stvarnu i efektivnu djelatnost u Mađarskoj jer je imalo zastupnika u Mađarskoj koji je naveden u slovačkom registru društava pod adresom koja se nalazi u Mađarskoj, otvorio je bankovni račun u Mađarskoj i raspolagao poštanskim pretincem te također obavljao aktivnosti u Mađarskoj putem internetskih stranica sastavljenih na mađarskom jeziku. Te su informacije ukazivale na postojanje poslovnog nastana, čime bi aktivnosti društva Weltimmo podlijevale mađarskom zakonu o zaštiti podataka i nadležnosti mađarskog nadzornog tijela. Međutim, SEU je nacionalnom sudu prepustio provjeru informacija i odluku o tome ima li Weltimmo poslovni nastan u Mađarskoj.

Ako bi sud koji je proslijedio predmet utvrdio da Weltimmo ima poslovni nastan u Mađarskoj, mađarsko bi nadzorno tijelo imalo ovlast izreći novčanu kaznu. S druge strane, ako bi nacionalni sud donio suprotnu odluku, odnosno da Weltimmo nema poslovni nastan u Mađarskoj, mjerodavni bi zakon bio zakon države članice (ili država članica) u kojoj je to društvo registrirano. Budući da se u tom slučaju ovlasti nadzornih tijela moraju izvršiti u skladu s teritorijalnim suverenitetom drugih država članica, mađarsko tijelo ne bi moglo izricati kazne. Budući da je Direktiva o zaštiti podataka sadržavala odredbu o sudjelovanju nadzornih tijela, mađarsko je tijelo moglo zatražiti od istovjetnog slovačkog tijela da ispita slučaj, utvrdi da je došlo do kršenja slovačkog zakona i izreče kazne propisane slovačkim zakonodavstvom.

S donošenjem OUZP-a uspostavljeni su detaljni propisi o nadležnosti nadzornih tijela u prekograničnim slučajevima. Uredbom je uspostavljen „jedinstveni mehanizam“ te su utvrđene odredbe o suradnji različitih nadzornih tijela. Radi učinkovite suradnje u prekograničnim slučajevima, OUZP-om se propisuje da vodeće nadzorno tijelo bude uspostavljeno kao nadzorno tijelo glavnog ili jedinog poslovnog nastana voditelja ili izvršitelja obrade⁵¹⁰. Vodeće nadzorno tijelo nadležno je za prekogranične predmete, jedini je sugovornik voditelja ili izvršitelja obrade te koordinira suradnju s drugim nadzornim tijelima kako bi se postigao konsenzus. Suradnja uključuje razmjenu informacija, uzajamnu pomoć u praćenju i vođenju istraga te donošenje obvezujućih odluka⁵¹¹.

U okviru prava Vijeća Europe, nadležnosti i ovlasti nadzornih tijela utvrđene su člankom 15. modernizirane Konvencije br. 108. Te ovlasti odgovaraju ovlastima koje su nadzornim tijelima dodijeljene pravom Unije, uključujući ovlasti za istraživanje i intervenciju, ovlasti za donošenje odluka i izricanje upravnih kazni za kršenje odredbi Konvencije te ovlasti za sudjelovanje u sudskim postupcima. Neovisna nadzorna tijela također su nadležna za obradu zahtjeva i pritužbi koje podnesu ispitanici, za podizanje svijesti javnosti o zakonodavstvu o zaštiti podataka te za savjetovanje nacionalnih donositelja odluka u vezi sa svim zakonodavnim ili upravnim mjerama kojima se regulira obrada osobnih podataka.

5.3. Suradnja

OUZP-om se uspostavlja opći okvir suradnje nadzornih tijela i utvrđuju konkretna pravila suradnje nadzornih tijela u prekograničnim aktivnostima obrade podataka.

Sukladno OUZP-u, nadzorna tijela pružaju si uzajamnu pomoć i dijele relevantne informacije radi dosljedne provedbe i primjene Uredbe⁵¹². To uključuje da nadzorno tijelo na zahtjev provodi savjetovanja, inspekcije i istrage. Nadzorna tijela mogu provoditi zajedničke operacije, uključujući zajedničke istrage i zajedničke mjere provedbe u kojima sudjeluje osoblje svih nadzornih tijela⁵¹³.

U EU-u voditelji obrade i izvršitelji obrade sve više djeluju na nadnacionalnoj razini. To zahtijeva blisku suradnju nadležnih nadzornih tijela u državama članicama kako

⁵¹⁰ Opća uredba o zaštiti podataka, članak 56. stavak 1.

⁵¹¹ *Ibid.*, članak 60.

⁵¹² *Ibid.*, članak 61. stavci od 1. do 3. i članak 62. stavak 1.

⁵¹³ *Ibid.*, članak 62. stavak 1.

bi se osiguralo da obrada osobnih podataka bude u skladu sa zahtjevima OUZP-a. Prema „jedinstvenom mehanizmu“ iz Uredbe, ako voditelj ili izvršitelj obrade ima poslovne nastane u nekoliko država članica ili ako ima jedan poslovni nastan, ali postupci obrade značajno utječu na ispitanike u više država članica, nadzorno tijelo glavnog (ili jedinog) poslovnog nastana vodeće je nadzorno tijelo za prekogranične aktivnosti voditelja ili izvršitelja obrade. Vodeća nadzorna tijela imaju ovlast poduzimanja provedbenih mjera protiv voditelja ili izvršitelja obrade. Cilj je jedinstvenog mehanizma poboljšati sukladnost i ujednačenu provedbu zakonodavstva EU-a o zaštiti podataka u različitim državama članicama. On je koristan i za poduzeća jer, zahvaljujući njemu, ona trebaju surađivati samo s vodećim nadzornim tijelom umjesto s nekoliko različitih nadzornih tijela. Time se povećava pravna sigurnost za poduzeća, a u praksi bi to također trebalo značiti da se odluke brže donose te da se poduzeća ne moraju nositi s proturječnim zahtjevima koja nameću različita nadzorna tijela.

Određivanje vodećeg nadzornog tijela podrazumijeva utvrđivanje lokacije glavnog poslovnog nastana poduzeća u EU-u. Pojam „glavnog poslovnog nastana“ definiran je u OUZP-u. Usto, Radna skupina iz članka 29. objavila je smjernice za utvrđivanje vodećeg nadzornog tijela ili izvršitelja obrade koje uključuju kriterije za određivanje glavnog poslovnog nastana⁵¹⁴.

Kako bi se osigurala visoka razina zaštite podataka u cijelom EU-u, vodeće nadzorno tijelo ne djeluje samostalno. Ono mora surađivati s drugim nadležnim nadzornim tijelima na donošenju odluka o obradi osobnih podataka koju obavljaju voditelji obrade i izvršitelji obrade kako bi se postigao konsenzus i osigurala dosljednost. Suradnja relevantnih nadzornih tijela uključuje razmjenu informacija, uzajamnu pomoć, provođenje zajedničkih istraga i aktivnosti praćenja⁵¹⁵. Prilikom pružanja uzajamne pomoći, nadzorna tijela moraju pravilno postupati sa zahtjevima za informacije koje upute druga nadzorna tijela te provoditi mjere nadzora, kao što su prethodno odobravanje i savjetovanje s voditeljem obrade podataka u vezi s njegovim aktivnostima obrade, inspekcije i istrage. Uzajamna pomoć nadzornim tijelima u drugim državama članicama mora se pružiti na zahtjev bez nepotrebne odgode i najkasnije u roku od mjesec dana nakon zaprimanja zahtjeva⁵¹⁶.

514 Radna skupina iz članka 29. (2016.), *Smjernice za identifikaciju voditelja obrade ili vodećeg nadzornog tijela izvršitelja obrade*, WP 244, Bruxelles, 13. prosinca 2016., revidirane 5. travnja 2017.

515 Opća uredba o zaštiti podataka, članak 60. stavci od 1. do 3.

516 *Ibid.*, članak 61. stavci 1. i 2.

Kada voditelj obrade ima poslovne nastane u nekoliko država članica, nadzorna tijela mogu provoditi zajedničke operacije, uključujući istrage i mjere provedbe u kojima sudjeluju članovi osoblja nadzornih tijela drugih država članica⁵¹⁷.

Suradnja različitih nadzornih tijela važan je zahtjev i prema pravu Vijeća Europe. Moderniziranom Konvencijom br. 108 utvrđuje se da nadzorna tijela moraju međusobno surađivati u mjeri potrebnoj za izvršavanje svojih zadaća⁵¹⁸. To se treba činiti, primjerice, razmjenom svih relevantnih i korisnih informacija, koordinacijom istraga i provođenjem zajedničkih aktivnosti⁵¹⁹.

5.4. Europski odbor za zaštitu podataka

Važnost neovisnih nadzornih tijela i glavne nadležnosti koje imaju prema europskom zakonodavstvu o zaštiti podataka opisane su u prethodnom dijelu ovog poglavlja. Europski odbor za zaštitu podataka (EOZP) drugi je važan dionik u osiguranju učinkovite i dosljedne primjene propisa o zaštiti podataka na razini EU-a.

OUZP-om je Odbor osnovan kao tijelo EU-a koje ima pravnu osobnost⁵²⁰. On je nasljednik Radne skupine iz članka 29.⁵²¹, koja je osnovana Direktivom o zaštiti podataka kako bi savjetovala Komisiju o svim mjerama EU-a koje utječu na prava pojedinaca u pogledu obrade osobnih podataka i privatnosti, promicala ujednačenu primjenu Direktive te Komisiji pružala stručna mišljenja o pitanjima povezanim sa zaštitom podataka. Radna skupina iz članka 29. sastojala se od predstavnika nadzornih tijela iz država članica EU-a te predstavnika Komisije i EDPS-a.

Slično kao i Radna skupina, EOZP čine voditelji nadzornih tijela iz svake države članice i EDPS-a ili njihovi predstavnici⁵²². EDPS ima jednaka prava glasa, uz iznimku predmeta koji su povezani s rješavanjem sporova, u kojima može glasovati samo o odlukama koje se odnose na načela i propise primjenjive na institucije EU-a koji

517 *Ibid.*, članak 62. stavak 1.

518 Modernizirana Konvencija br. 108, članci 16. i 17.

519 *Ibid.*, članak 17.

520 Opća uredba o zaštiti podataka, članak 68.

521 Sukladno Direktivi 95/46/EZ, Radna skupina iz članka 29. trebala je savjetovati Komisiju o svim mjerama EU-a koje utječu na prava pojedinaca u pogledu obrade osobnih podataka i privatnosti, promicati ujednačenu primjenu Direktive te pružati stručna mišljenja Komisiji o pitanjima povezanim sa zaštitom podataka. Radna skupina iz članka 29. sastojala se od predstavnika nadzornih tijela iz država članica EU-a, Komisije i EDPS-a.

522 Opća uredba o zaštiti podataka, članak 68. stavak 3.

su u suštini sukladni onima iz OUZP-a. Komisija ima pravo sudjelovanja u aktivnostima i sastancima Odbora, no nema pravo glasa⁵²³. Odbor izabire predsjednika (koji je ujedno predstavnik Odbora) i dva zamjenika predsjednika iz redova svojih članova natpolovičnom većinom na razdoblje od pet godina. EOZP također ima tajništvo koje osigurava Europski nadzornik za zaštitu podataka radi analitičke, administrativne i logističke potpore Odboru⁵²⁴.

Zadaće EOZP-a detaljno su navedene u člancima 64., 65. i 70. Opće uredbe o zaštiti podataka, a uključuju sveobuhvatne dužnosti koje se mogu podijeliti u tri glavne aktivnosti:

- **Dosljednost:** EOZP može donositi pravno obvezujuće odluke u trima slučajevima: ako nadzorno tijelo podnese relevantan i obrazložen prigovor kad je riječ o jedinstvenim kontaktnim točkama, ako postoje oprečna stajališta o tome koje je nadzorno tijelo „vodeće” te, naposljetku, ako nadležno nadzorno tijelo ne zatraži ili ne uzme u obzir mišljenje EOZP-a⁵²⁵. Glavna je odgovornost EOZP-a osigurati dosljednu provedbu Uredbe na razini EU-a te on igra ključnu ulogu u mehanizmu konzistentnosti, koji je opisan u [dijelu 5.5](#).
- **Savjetovanje:** zadaće EOZP-a uključuju savjetovanje Komisije o svim pitanjima u pogledu zaštite osobnih podataka u Uniji, poput izmjena OUZP-a, revizija zakonodavstva EU-a koje se odnosi na obradu podataka i koje može biti u sukobu s propisima EU-a o zaštiti podataka, ili izdavanja Komisijinih odluka o primjerenosti koje omogućuju prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama.
- **Smjernice:** Odbor također izdaje smjernice, preporuke i primjere najbolje prakse kako bi potaknuo dosljednu provedbu Uredbe te promiče suradnju i razmjenu znanja među nadzornim tijelima. Usto mora poticati udruženja voditelja obrade ili izvršitelja obrade da izrađuju kodekse ponašanja te uspostave mehanizme certificiranja i pečata za zaštitu podataka.

Odluke EOZP-a mogu se osporiti pred SEU-om.

523 *Ibid.*, članak 68. stavci 4. i 5.

524 *Ibid.*, članci 73. i 75.

525 *Ibid.*, članak 65.

5.5. Mehanizam konzistentnosti iz Opće uredbe o zaštiti podataka

OUZP-om se uspostavlja mehanizam konzistentnosti kojim se osigurava da se Uredba dosljedno provodi u svim državama članicama putem međusobne suradnje nadzornih tijela i, po potrebi, njihove suradnje s Komisijom. Mehanizam konzistentnosti primjenjuje se u dvama slučajevima. Prvi se slučaj odnosi na mišljenja EOZP-a u slučajevima u kojima nadzorno tijelo namjerava donijeti mjere poput popisa postupaka obrade koji zahtijevaju procjenu učinka zaštite podataka (DPIA) ili određivanja standardnih ugovornih klauzula. Drugi se slučaj odnosi na obvezujuće odluke EOZP-a za nadzorna tijela u slučajevima jedinstvene kontaktne točke i kada nadzorno tijelo ne uzima u obzir ili ne zatraži mišljenje EOZP-a.

6

Prava ispitanika i njihova provedba

EU	Obuhvaćena pitanja	Vijeće Europe
Pravo na informacije		
Opća uredba o zaštiti podataka, članak 12. SEU, C-473/12, <i>Institut professionnel des agents immobiliers (IPI) protiv Engleberta</i> , 2013. SEU, C-201/14, <i>Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.</i> , 2015.	Transparentnost informacija	Modernizirana Konvencija br. 108, članak 8.
Opća uredba o zaštiti podataka, članak 13. stavci 1. i 2. i članak 14. stavci 1. i 2.	Sadržaj informacija	Modernizirana Konvencija br. 108, članak 8. stavak 1.
Opća uredba o zaštiti podataka, članak 13. stavak 1. i članak 14. stavak 3.	Vrijeme pružanja informacija	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (b).
Opća uredba o zaštiti podataka, članak 12. stavci 1., 5. i 7.	Način pružanja informacija	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (b).
Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (d), članak 14. stavak 2. točka (e) te članci 77., 78. i 79.	Pravo na podnošenje pritužbe	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (f)

EU	Obuhvaćena pitanja	Vijeće Europe
Pravo na pristup		
Opća uredba o zaštiti podataka, članak 15. stavak 1. SEU, C-553/07, <i>College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer</i> , 2009. SEU, spojeni predmeti C-141/12 i C-372/12, <i>Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.</i> , 2014. SEU, C-434/16, <i>Peter Nowak protiv Data Protection Commissioner</i> , 2017.	Pravo na pristup vlastitim podacima	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (b) ESLJP, <i>Leander protiv Švedske</i> , br. 9248/81, 1987.
Pravo na ispravak		
Opća uredba o zaštiti podataka, članak 16.	Ispravak netočnih osobnih podataka	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (e) ESLJP, <i>Cemalettin Canli protiv Turske</i> , br. 22427/04, 2008. ESLJP, <i>Ciubotaru protiv Moldavije</i> , br. 27138/04, 2010.
Pravo na brisanje		
Opća uredba o zaštiti podataka, članak 17. stavak 1.	Brisanje osobnih podataka	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (e) ESLJP, <i>Segetstedt-Wiberg i drugi protiv Švedske</i> , br. 62332/00, 2006.
SEU, C-131/12, <i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González [VV]</i> , 2014. SEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija</i> , 2017.	Pravo na zaborav	

EU	Obuhvaćena pitanja	Vijeće Europe
Pravo na ograničenje obrade		
Opća uredba o zaštiti podataka, članak 18. stavak 1.	Pravo na ograničenje uporabe osobnih podataka	
Opća uredba o zaštiti podataka, članak 19.	Obveza obavješćivanja	
Pravo na prenosivost podataka		
Opća uredba o zaštiti podataka, članak 20.	Pravo na prenosivost podataka	
Pravo na prigovor		
Opća uredba o zaštiti podataka, članak 21. stavak 1. SEU, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija</i> , 2017.	Pravo na prigovor zbog posebne situacije ispitanika	Preporuka o izradi profila, članak 5.3. Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (d)
Opća uredba o zaštiti podataka, članak 21. stavak 2.	Pravo na prigovor na uporabu podataka u marketinške svrhe	Preporuka o direktnom marketingu, članak 4.1.
Opća uredba o zaštiti podataka, članak 21. stavak 5.	Pravo na prigovor automatiziranim putem	
Prava povezana s automatiziranim donošenjem odluka i izradom profila		
Opća uredba o zaštiti podataka, članak 22.	Prava povezana s automatiziranim donošenjem odluka i izradom profila	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (a)
Opća uredba o zaštiti podataka, članak 21.		
Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (f)	Pravo na prigovor na automatizirano donošenje odluka Prava na smisleno pojašnjenje	Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (c)

EU	Obuhvaćena pitanja	Vijeće Europe
Pravni lijekovi, odgovornost, sankcije i naknada		
Povelja, članak 47. SEU, C-362/14, <i>Maximillian Schrems protiv Data Protection Commissioner</i> [VV], 2015. Opća uredba o zaštiti podataka, članci od 77. do 84.	Za kršenja nacionalnog zakonodavstva o zaštiti podataka	Europska konvencija o ljudskim pravima, članak 13. (samo za države članice Vijeća Europe) Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (f) te članci 12., 15. i od 16. do 21. ESLJP, <i>K. U. protiv Finske</i>, br. 2872/02, 2008. ESLJP, <i>Biriuk protiv Litve</i>, br. 23373/03, 2008.
Uredba o zaštiti podataka u institucijama Europske unije, članci 34. i 49. SEU, C-28/08 P, <i>Europska komisija protiv The Bavarian Lager Co. Ltd</i> [VV], 2010.	Za kršenja prava Europske unije od strane institucija i tijela Europske unije	

Učinkovitost pravnih propisa općenito, a posebno prava ispitanika, u velikoj mjeri ovisi o postojanju odgovarajućih mehanizama za njihovu provedbu. U digitalnom dobu obrada podataka postala je sveprisutna i prosječna je osoba sve teže razumije. Kako bi se umanjila neravnoteža moći između ispitanika i voditelja obrade, pojedinci imaju određena prava koja im omogućuju ostvarenje veće kontrole nad obradom njihovih osobnih podataka. Pravo na pristup vlastitim podacima i pravo na njihov ispravak zajamčena su člankom 8. stavkom 2. Povelje EU-a o temeljnim pravima, dokumenta koji čini primarno pravo Unije i temelj je pravnog poretka EU-a. Sekundarnim pravom Unije, a posebice Općom uredbom o zaštiti podataka, uspostavlja se usklađen pravni okvir koji ispitanicima na raspolaganje stavlja prava povezana s voditeljima obrade. Uz pravo na pristup i ispravak, OUZP-om se utvrđuje niz drugih prava, poput prava na brisanje („pravo na zaborav“), prava na prigovor ili na ograničenje obrade podataka te prava povezanih s automatiziranim donošenjem odluka i izradom profila. Slične zaštitne mjere putem kojih ispitanici mogu preuzeti kontrolu nad svojim podacima utvrđene su i u moderniziranoj Konvenciji br. 108. U članku 9. navedena su prava koja pojedinci trebaju imati na raspolaganju u vezi s obradom njihovih osobnih podataka. Ugovorne stranke moraju osigurati da su ta prava dostupna svakom ispitaniku u njihovu području nadležnosti te da su ona popraćena djelotvornim pravnim i praktičnim mjerama kako bi ih ispitanici mogli ostvariti.

Uz pružanje prava pojedincima, jednako je važno uspostaviti mehanizme koji ispitanicima omogućuju da ulože prigovor na kršenje svojih prava, pozovu voditelje obrade na odgovornost i zatraže naknadu štete. Pravo na učinkovit pravni lijek, zajamčen EKLJP-om i Poveljom, podrazumijeva da su pravni lijekovi dostupni svakoj osobi.

6.1. Prava ispitanika

Ključne točke

- Svaki ispitanik ima pravo na informacije o svakoj obradi koju voditelj obrade podataka vrši na njegovim osobnim podacima, uz određena ograničenja izuzeća.
- Ispitanici imaju pravo na:
 - pristup vlastitim podacima i dobivanje određenih informacija o njihovoj obradi,
 - ispravak svojih podataka, ako su netočni, koji provodi voditelj obrade koji ih obrađuje,
 - brisanje svojih podataka koje po potrebi provodi voditelj obrade ako podatke obrađuje nezakonito,
 - privremeno ograničenje obrade,
 - prijenos svojih podataka drugom voditelju obrade u određenim uvjetima.
- Osim toga, ispitanici imaju pravo na prigovor na obradu s obzirom na:
 - osnovu koja se odnosi na njihovu posebnu situaciju,
 - uporabu njihovih podataka u svrhu izravnog marketinga.
- Ispitanici imaju pravo na to da se o njima ne donose odluke koje se temelje isključivo na automatiziranoj obradi, uključujući izradu profila, a koje imaju pravni učinak ili koje značajno utječu na njih. Ispitanici također imaju pravo na:
 - ljudsku intervenciju voditelja obrade,
 - izražavanje vlastitog stajališta te osporavanje odluke koja se temelji na automatiziranoj obradi.

6.1.1. Pravo na informacije

Prema **pravu Vijeća Europe** i **pravu EU-a**, voditelji postupaka obrade dužni su obavijestiti ispitanika o svrsi obrade u trenutku prikupljanja osobnih podataka. Ta obveza ne ovisi o zahtjevu ispitanika, nego voditelj obrade mora proaktivno ispunjavati tu obvezu, neovisno o tome pokazuje li ispitanik interes za informacije ili ne.

Prema pravu Vijeća Europe, sukladno članku 8. modernizirane Konvencije br. 108, ugovorne stranke moraju osigurati da voditelji obrade obavijeste ispitanike o svojem identitetu i uobičajenom boravištu, pravnoj osnovi i svrsi obrade, kategorijama osobnih podataka koji se obrađuju, primateljima njihovih osobnih podataka (ako postoje) te o tome kako mogu ostvariti svoja prava na temelju članka 9., koja uključuju pravo na pristup, ispravak i pravni lijek. Ispitanicima se trebaju priopćiti i sve druge dodatne informacije koje se smatraju nužnima za poštenu i transparentnu obradu osobnih podataka. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 pojašnjava se da informacije koje se pružaju ispitanicima „trebaju biti jednostavno dostupne, čitljive, razumljive i prilagođene relevantnim ispitanicima”⁵²⁶.

U sklopu prava Unije, načelo transparentnosti podrazumijeva da svaka obrada osobnih podataka općenito treba biti transparentna za pojedince. Pojedinci imaju pravo znati kako se i koji osobni podaci prikupljaju, upotrebljavaju ili drugačije obrađuju te koji su rizici, zaštitne mjere i njihova prava u vezi s obradom⁵²⁷. Člankom 12. OUZP-a utvrđuje se široka sveobuhvatna obveza za voditelje obrade prema kojoj moraju pružiti transparentne informacije i/ili priopćiti ispitanicima kako mogu ostvariti svoja prava⁵²⁸. Informacije moraju biti sažete, transparentne, razumljive i lako dostupne te pružene na jasnom i jednostavnom jeziku. Informacije se moraju pružiti u pisanom obliku, uključujući elektroničkim putem ako je prikladno, a na zahtjev ispitanika mogu se pružiti i usmenim putem, pod uvjetom da je bez sumnje utvrđen njegov identitet. Informacije se pružaju bez prekomjerne odgode ili naknade⁵²⁹.

Članci 13. i 14. OUZP-a odnose se na pravo ispitanika na informacije u slučajevima u kojima su osobni podaci prikupljeni izravno od njih odnosno slučajevima u kojima nisu dobiveni od njih.

⁵²⁶ Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 68.

⁵²⁷ Opća uredba o zaštiti podataka, uvodna izjava 39.

⁵²⁸ *Ibid.*, članci 13. i 14.; modernizirana Konvencija br. 108, članak 8. stavak 1. točka (b).

⁵²⁹ Opća uredba o zaštiti podataka, članak 12. stavak 5.; modernizirana Konvencija br. 108, članak 9. stavak 1. točka (b).

Opseg prava na informacije i njegova ograničenja na temelju prava Unije pojašnjeni su u sudskoj praksi SEU-a.

Primjer: U predmetu *Institut professionnel des agents immobiliers (IPI) protiv Engleberta*⁵³⁰ od SEU-a se tražilo da tumači članak 13. stavak 1. Direktive 95/46/EZ. Tim je člankom državama članicama pružena mogućnost izbora o donošenju zakonskih mjera za ograničavanje područja primjene prava ispitanika na informacije kada je to potrebno radi, među ostalim, zaštite prava i sloboda drugih te sprečavanja i istrage kaznenih djela ili kršenja etike zakonom uređenih djelatnosti. IPI je strukovna organizacija agenata za nekretnine u Belgiji koja je odgovorna za osiguranje sukladnosti s odgovarajućim praksama djelatnosti prodaje nekretnina. Ona je od nacionalnog suda zatražila da presudi da su optuženici prekršili pravila djelatnosti i da im naredi da obustave aktivnosti prodaje nekretnina. Postupak je pokrenut na temelju dokaza koje su prikupili privatni istražitelji koje je IPI zaposlio.

Nacionalni je sud imao sumnji u vezi s vrijednošću dokaza koje su dostavili istražitelji s obzirom na mogućnost da su prikupljeni bez poštovanja propisa o zaštiti podataka iz belgijskog zakonodavstva, a posebice obveze da se ispitanike obavijesti o obradi njihovih osobnih podataka prije prikupljanja takvih informacija. SEU je istaknuo da je u članku 13. stavku 1. utvrđeno da države članice „mogu“, no ne moraju propisati iznimke u svojim nacionalnim zakonodavstvima za obvezu obavješćivanja ispitanika o obradi njihovih podataka. Budući da članak 13. stavak 1. uključuje sprečavanje, istragu, otkrivanje i progono kaznenih djela ili kršenje etike kao osnove po kojima države članice mogu ograničiti prava pojedinaca, aktivnost tijela poput IPI-ja i privatnih istražitelja koji djeluju u njegovo ime može se temeljiti na toj odredbi. Međutim, ako država članica nije propisala takvu iznimku, ispitanike se mora obavijestiti.

Primjer: U predmetu *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*⁵³¹ SEU je obrazložio sprečava li se pravom EU-a prijenos osobnih podataka jednog nacionalnog tijela javne uprave drugom tijelu javne uprave radi daljnje obrade bez obavješćivanja ispitanika o prijenosu

530 SEU, C-473/12, *Institut professionnel des agents immobiliers (IPI) protiv Geoffreyja Engleberta i dr.*, 7. studenoga 2013.

531 SEU, C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. listopada 2015.

i o obradi. U tom predmetu Državna agencija za upravljanje nije obavijestila tužitelje da je prenijela njihove podatke Državnom fondu za socijalnu sigurnost prije samog prijenosa.

SEU je smatrao da je zahtjev iz prava Unije za obavješćavanje ispitanika o obradi njihovih osobnih podataka „tim važniji zato što je riječ o nužnoj pretpostavci za to da te osobe koriste svoje pravo na pristup i ispravljanje obrađenih podataka [...] i svoje pravo prigovora obradi spomenutih podataka“. Prema načelu poštene obrade zahtijeva se obavješćavanje ispitanika o prijenosu njihovih podataka drugom javnom tijelu radi daljnje obrade. Sukladno članku 13. stavku 1. Direktive 95/46/EZ, države članice mogu ograničiti pravo na informacije ako se to smatra nužnim za zaštitu važnog gospodarskog interesa države, uključujući porezna pitanja. Međutim, takva se ograničenja moraju provesti zakonskim mjerama. Budući da ni definicija podataka koji se prenose ni detaljni načini prijenosa nisu utvrđeni zakonskom mjerom, nego isključivo protokolom između dvaju javnih tijela, uvjeti za odstupanje na temelju prava Unije nisu ispunjeni. Tužitelji su trebali biti unaprijed obaviješteni o prijenosu njihovih podataka Državnom fondu za socijalnu sigurnost te o naknadnoj obradi podataka u tom tijelu.

Sadržaj informacija

Sukladno članku 8. stavku 1. modernizirane Konvencije br. 108, voditelj obrade dužan je pružiti ispitaniku sve informacije kojima se osigurava poštena i transparentna obrada osobnih podataka, uključujući sljedeće:

- identitet i uobičajeno boravište ili poslovni nastan voditelja obrade,
- pravnu osnovu i predviđene svrhe obrade,
- kategorije obrađenih osobnih podataka,
- primatelje ili kategorije primatelja osobnih podataka, ako ih ima,
- načine na koje ispitanici mogu ostvariti svoja prava.

Sukladno OUP-u, ako su osobni podaci prikupljeni od ispitanika, voditelj obrade dužan je u trenutku prikupljanja osobnih podataka pružiti ispitaniku sljedeće informacije⁵³²:

- identitet i kontaktne podatke voditelja obrade i, ako je primjenjivo, službenika za zaštitu podataka voditelja obrade,
- svrhu obrade i pravnu osnovu za obradu, tj. ugovorna ili zakonska obveza,
- legitimni interes voditelja obrade podataka ako on čini osnovu za obradu,
- krajnje primatelje ili kategorije primatelja osobnih podataka,
- hoće li se osobni podaci prenijeti trećoj zemlji ili međunarodnoj organizaciji te temelji li se izbor na odluci o primjerenosti ili odgovarajućim zaštitnim mjerama,
- razdoblje u kojem će osobni podaci biti pohranjeni ili, ako nije moguće odrediti razdoblje, kriterije prema kojima se utvrdilo razdoblje pohrane podataka,
- prava ispitanika u vezi s obradom, poput prava na pristup osobnim podacima, prava na ispravak, brisanje ili ograničavanje obrade podataka ili prava na prigovor na obradu,
- je li pružanje osobnih podataka zakonska ili ugovorna obveza, ima li ispitanik obvezu pružanja osobnih podataka te koje su moguće posljedice ako se takvi podaci ne pruže,
- postojanje automatiziranog donošenja odluka, uključujući izradu profila,
- pravo na podnošenje pritužbe nadzornom tijelu,
- postojanje prava na povlačenje privole.

U slučajevima automatiziranog donošenja odluka, uključujući izradu profila, ispitanici moraju primiti smislene informacije o logici izrade profila, njezinoj važnosti i predviđenim posljedicama takve obrade.

⁵³² Opća uredba o zaštiti podataka, članak 13. stavak 1.

U slučajevima u kojima osobni podaci nisu dobiveni izravno od ispitanika, voditelj obrade podataka mora obavijestiti pojedinca o podrijetlu osobnih podataka. U svakom slučaju voditelj obrade mora, među ostalim, obavijestiti ispitanike o postojanju automatiziranog donošenja odluka, uključujući izradu profila⁵³³. Naposljetku, ako voditelj obrade namjerava obrađivati osobne podatke u svrhu koja je različita od one koja je izvorno navedena ispitaniku, prema načelima ograničenja svrhe i transparentnosti od voditelja obrade se zahtijeva da ispitaniku pruži informacije o toj novoj svrsi. Voditelji obrade moraju pružiti informacije prije bilo kakve daljnje obrade. Drugim riječima, u slučajevima u kojima je ispitanik dalo privolu za obradu osobnih podataka voditelj obrade mora primiti novu privolu ispitanika ako se promijeni svrha obrade ili se dodaju nove svrhe.

Vrijeme pružanja informacija

U OUZP-u se razlikuju dvije situacije i dva trenutka u kojima voditelj obrade podataka mora pružiti informacije ispitaniku.

- Ako su osobni podaci prikupljeni izravno od ispitanika, voditelj obrade u trenutku prikupljanja podataka toj osobi mora pružiti sve relevantne informacije i prava koja ima na temelju OUZP-a⁵³⁴.

Ako voditelj obrade namjerava dodatno obrađivati osobne podatke u drugu svrhu, prije te dodatne obrade pruža sve relevantne informacije o tome.

- Ako osobni podaci nisu dobiveni od ispitanika, voditelj obrade dužan je ispitaniku pružiti informacije o obradi „unutar razumnog roka nakon dobivanja osobnih podataka, a najkasnije u roku od jednog mjeseca” ili prije otkrivanja podataka trećoj strani⁵³⁵.

U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 utvrđuje se da ako obavješćivanje ispitanika nije moguće u trenutku započinjanja obrade, ono se može izvršiti u kasnijoj fazi, primjerice, kada voditelj obrade zbog bilo kojeg razloga stupi u kontakt s ispitanikom⁵³⁶.

533 *Ibid.*, članak 13. stavak 2. i članak 14. stavak 2. točka (f).

534 *Ibid.*, članak 13. stavci 1. i 2., uvod u kojemu se tekst Uredbe odnosi na obvezne informacije koje se moraju primijeniti „u trenutku prikupljanja osobnih podataka”.

535 *Ibid.*, članak 13. stavak 3. i članak 14. stavak 3.; vidjeti i upućivanje na razumne rokove i izbjegavanje nepotrebnog odgađanja na temelju modernizirane Konvencije br. 108, članak 8. stavak 1. točka (b).

536 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 70.

Različiti načini pružanja informacija

Prema pravu Vijeća Europe i EU-a, informacije koje je voditelj obrade dužan pružiti ispitanicima moraju biti sažete, transparentne, razumljive i lako dostupne. Moraju se pružiti u pisanom obliku ili drugim sredstvima, uključujući elektroničkim putem, uz uporabu jasnog, jednostavnog i lako razumljivog jezika. Prilikom pružanja informacija voditelj obrade može upotrijebiti standardizirane ikone kako bi informacije bile dostupne na lako vidljiv i razumljiv način⁵³⁷. Primjerice, ikona koja izgleda kao lokot može se upotrijebiti kao oznaka sigurnog prikupljanja i/ili šifriranja podataka. Ispitanici mogu zatražiti da im se informacije pruže usmeno. Informacije se moraju pružati bez naknade, osim ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani (npr. zbog njihova učestalog ponavljanja)⁵³⁸. Jednostavan pristup pruženim informacijama neophodan je za ostvarivanje prava ispitanika, koja su osigurana zakonodavstvom EU-a o zaštiti podataka.

Načelom poštene obrade propisuje se da informacije moraju biti lako razumljive ispitanicima. Mora se upotrebljavati jezik koji odgovara primateljima. Razina i vrsta upotrijebljenog jezika mora se razlikovati ovisno o tome jesu li informacije namijenjene, na primjer, odraslima ili djeci, široj javnosti ili stručnom akademskom osoblju. Pitanje uravnoteživanja aspekta razumljivih informacija razmatra se u Mišljenju Radne skupine iz članka 29. o usklađenijem pružanju informacija. Njime se promiče ideja takozvanih „slojevitih obavijesti”⁵³⁹ koje ispitaniku omogućuju da odluči o željenoj razini detalja. Međutim, takvim se načinom pružanja informacija voditelja obrade ne oslobađa obveze koje ima na temelju članaka 13. i 14. OUZP-a. Voditelj obrade i dalje je dužan pružiti ispitaniku sve informacije.

Jedan je od najučinkovitijih načina pružanja informacija postavljanje odgovarajućih informacijskih klauzula na naslovnici internetske stranice voditelja obrade, kao što su pravila zaštite privatnosti internetske stranice. Međutim, znatan dio stanovništva ne služi se internetom, što bi društvo ili javno tijelo trebalo uzeti u obzir u svojim pravilima informiranja.

537 Europska komisija dodatno će razviti informacije koje se prikazuju ikonama i postupke za utvrđivanje standardiziranih ikona putem delegiranih akata; vidjeti Opću uredbu o zaštiti podataka, članak 12. stavak 8.

538 Opća uredba o zaštiti podataka, članak 12. stavci 1., 5. i 7., te modernizirana Konvencija br. 108, članak 9. stavak 1. točka (b).

539 Radna skupina iz članka 29. (2004.), *Mišljenje 10/2004 o usklađenijem pružanju informacija*, WP 100, Bruxelles, 25. studenoga 2004.

Obavijest o zaštiti privatnosti koja se odnosi na obradu osobnih podataka na internetskoj stranici mogla bi izgledati kako slijedi:

Tko smo mi?

„Voditelj obrade” podataka jest društvo Bed and Breakfast C&U sa sjedištem na adresi [adresa: xxx], tel.: xxx; faks: xxx; e-pošta: info@c&u.com; kontaktni podaci službenika za zaštitu podataka: [xxx].

Obavijest s informacijama o osobnim podacima čini dio uvjeta i odredbi kojima su uređene naše hotelske usluge.

Koje podatke prikupljamo od vas?

Od vas prikupljamo sljedeće osobne podatke: vaše ime, poštansku adresu, telefonski broj, adresu e-pošte, informacije o boravku, broj kreditne i debitne kartice te IP adrese ili nazive domena računala putem kojih ste posjetili našu internetsku stranicu.

Zašto prikupljamo vaše podatke?

Obradujemo vaše podatke na temelju vaše privole i u svrhe rezervacija, sklapanja i izvršavanja ugovora u vezi s uslugama koje vam pružamo te radi ispunjavanja svojih zakonskih obveza, primjerice odredbi Zakona o lokalnim pristojbama, prema kojima moramo prikupljati osobne podatke kako bismo mogli naplatiti gradski porez za smještaj.

Kako obrađujemo vaše podatke?

Vaše ćemo osobne podatke čuvati tri mjeseca. Vaši podaci ne podvrgavaju se postupcima automatiziranog donošenja odluka.

Društvo Bed and Breakfast C&U pridržava se strogih sigurnosnih postupaka kako bi osiguralo da se vaši osobni podaci ne oštete, ne unište i ne otkriju trećoj strani bez vašeg dopuštenja te kako bi se spriječio neovlašten pristup njima. Računala na kojima se pohranjuju informacije smještene su u sigurna okruženja s ograničenim fizičkim pristupom. Upotrebljavamo

sigurne vatrozide i druge mjere za ograničenje elektroničkog pristupa. Ako se podaci moraju prenijeti trećoj strani, od nje zahtijevamo da ima uspostavljene slične mjere za zaštitu vaših osobnih podataka.

Sve informacije koje prikupimo ili evidentiramo ograničene su na naše poslovne prostore. Osobnim podacima smiju pristupiti samo osobe kojima su te informacije nužne za ispunjavanje ugovornih obveza. Izričito ćemo vas pitati kada su nam potrebne informacije o vašem identitetu. Možda ćemo od vas tražiti da sudjelujete u našim sigurnosnim provjerama prije nego što vam otkrijemo informacije. Osobne podatke koje nam pružite možete izmijeniti u bilo kojem trenutku tako da nam se izravno obratite.

Koja su vaša prava?

Imate pravo na pristup svojim podacima, pravo dobiti primjerak svojih podataka, zatražiti njihovo brisanje ili ispravak ili zatražiti prijenos svojih podataka drugom voditelju obrade.

Svoje zahtjeve možete poslati na adresu info@c&u.com. Dužni smo odgovoriti na vaš zahtjev unutar mjesec dana, no ako je on previše složen ili ako zaprimimo previše drugih zahtjeva, obavijestit ćemo vas da se to razdoblje može produljiti za dodatna dva mjeseca.

Pristup vašim osobnim podacima

Imate pravo pristupiti svojim podacima, na zahtjev dobiti informacije o razlozima za njihovu obradu, zatražiti njihovo brisanje ili ispravak te ne sudjelovati u potpuno automatiziranom postupku donošenja odluka bez uzimanja u obzir vašeg mišljenja. Svoje zahtjeve možete poslati na adresu info@c&u.com. Također imate pravo na prigovor na obradu, pravo povući privolu i podnijeti pritužbu nacionalnom nadzornom tijelu ako smatrate da se obradom podataka krši zakon te zatražiti odštetu za štetu nastalu zbog nezakonite obrade.

Pravo na podnošenje pritužbe

OUZP-om se od voditelja obrade zahtijeva da obavijesti ispitanike o mehanizmima provedbe na temelju nacionalnog prava i prava Unije u slučajevima povrede osobnih podataka. Voditelj obrade mora obavijestiti ispitanike o njihovu pravu na podnošenje

pritužbe zbog povrede osobnih podataka nadzornom tijelu ili, po potrebi, nacionalnom sudu⁵⁴⁰. Pravom Vijeća Europe također se propisuje pravo ispitanika na informacije o načinima ostvarivanja njihovih prava, uključujući pravo na pravni lijek utvrđeno člankom 9. stavkom 1. točkom (f).

Izuzeća od obveze obavješćivanja

OUZP-om se utvrđuje izuzeće od obveze obavješćivanja. Sukladno članku 13. stavku 4. i članku 14. stavku 5. OUZP-a, obveza obavješćivanja ispitanika ne primjenjuje se ako oni već posjeduju sve relevantne informacije⁵⁴¹. Usto, ako osobni podaci nisu dobiveni od ispitanika, obveza obavješćivanja ne primjenjuje se ako je pružanje informacija nemoguće ili nerazmjerno, posebno ako se osobni podaci obrađuju u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe⁵⁴².

Nadalje, prema OUZP-u, države članice imaju diskrecijsku ovlast ograničiti obveze i prava pojedinaca na temelju Uredbe ako to predstavlja nužnu i razmjernu mjeru u demokratskom društvu, primjerice za zaštitu nacionalne ili javne sigurnosti, obranu, zaštitu pravosudnih istraga i postupaka ili zaštitu gospodarskih ili financijskih interesa te privatnih interesa koji su važniji od interesa zaštite podataka⁵⁴³.

Sva izuzeća ili ograničenja moraju biti nužna u demokratskom društvu i razmjerna cilju koji se nastoji ostvariti. U vrlo iznimnim slučajevima, primjerice zbog medicinskih razloga, zaštita ispitanika može zahtijevati ograničenje transparentnosti, što se posebno odnosi na ograničenje prava na pristup svakog ispitanika⁵⁴⁴. Međutim, kao minimalna razina zaštite, nacionalnim zakonodavstvom mora se poštovati bit temeljnih prava i sloboda zaštićenih pravom Unije⁵⁴⁵. Za to je potrebno da nacionalno zakonodavstvo sadržava posebne odredbe kojima se pojašnjavaju svrha obrade, kategorije obuhvaćenih osobnih podataka, zaštitne mjere i drugi postupovni zahtjevi⁵⁴⁶.

540 Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (d) i članak 14. stavak 2. točka (e); modernizirana Konvencija br. 108, članak 8. stavak 1. točka (f).

541 Opća uredba o zaštiti podataka, članak 13. stavak 4. i članak 14. stavak 5. točka (a).

542 *Ibid.*, članak 14. stavak 5. točke od (b) do (e).

543 *Ibid.*, članak 23. stavak 1.

544 *Ibid.*, članak 15.

545 *Ibid.*, članak 23. stavak 1.

546 *Ibid.*, članak 23. stavak 2.

Ako se osobni podaci prikupljaju u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u javnom interesu, pravom Unije ili države članice mogu se predvidjeti odstupanja od obveze obavješćivanja ako je vjerojatno da bi se time moglo onemogućiti ili ozbiljno ugroziti postizanje tih posebnih svrha⁵⁴⁷.

Slična ograničenja javljaju se i u okviru prava Vijeća Europe te se prava dodijeljena ispitanicima na temelju članka 9. modernizirane Konvencije br. 108 mogu podvrgnuti mogućim ograničenjima iz članka 11. modernizirane Konvencije br. 108 u strogim uvjetima. Osim toga, sukladno članku 8. stavku 2. modernizirane Konvencije br. 108, obveza transparentnosti obrade podataka koja se nameće voditeljima obrade ne primjenjuje se ako ispitanik već posjeduje te informacije.

Pravo pojedinca na pristup vlastitim podacima

Unutar prava Vijeća Europe, pravo pojedinca na pristup vlastitim podacima izričito je potvrđeno člankom 9. modernizirane Konvencije br. 108. Njime se utvrđuje da svaki pojedinac ima pravo na zahtjev dobiti informacije o obradi osobnih podataka koji se odnose na njega, i to na razumljiv način. Pravo na pristup nije priznato samo odredbama modernizirane Konvencije br. 108, nego i sudskom praksom ESLJP-a. ESLJP je opetovano tvrdio da pojedinci imaju pravo na pristup informacijama o vlastitim osobnim podacima te da to pravo proizlazi iz potrebe za poštovanjem privatnog života⁵⁴⁸. Međutim, pravo na pristup osobnim podacima koje čuvaju javne ili privatne organizacije može biti ograničeno u određenim okolnostima⁵⁴⁹.

Unutar prava EU-a, pravo na pristup vlastitim podacima izričito je potvrđeno u članku 15. OUZP-a, a navedeno je i kao element temeljnog prava na zaštitu osobnih podataka u članku 8. stavku 2. Povelje EU-a o temeljnim pravima⁵⁵⁰. Pravo pojedinca na pristup vlastitim osobnim podacima ključan je element europskog zakonodavstva o zaštiti podataka⁵⁵¹.

547 *Ibid.*, članak 89. stavci 2. i 3.

548 ESLJP, *Gaskin protiv Ujedinjene Kraljevine*, br. 10454/83, 7. srpnja 1989.; ESLJP, *Odièvre protiv Francuske* [VV], br. 42326/98, 13. veljače 2003.; ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 28. travnja 2009.; ESLJP, *Godelli protiv Italije*, br. 33783/09, 25. rujna 2012.

549 ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.

550 Vidjeti i SEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. srpnja 2014.; SEU, C-615/13 P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA)*, Europska komisija, 16. srpnja 2015.

551 SEU, spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. srpnja 2014.

OUZP-om se propisuje da svaki ispitanik ima pravo na pristup svojim osobnim podacima i na određene informacije o obradi, koje voditelji obrade moraju pružiti⁵⁵². Svaki ispitanik posebno ima pravo dobiti potvrdu (voditelja obrade) o tome obrađuju li se njegovi podaci te barem informacije o sljedećem:

- svrhama obrade,
- kategorijama osobnih podataka o kojima je riječ,
- primateljima ili kategorijama primatelja kojima se osobni podaci otkrivaju,
- predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja,
- postojanju prava na ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka,
- pravu na podnošenje pritužbe nadzornom tijelu,
- svakoj dostupnoj informaciji o izvoru podataka koji se obrađuju ako se podaci ne prikupljaju od ispitanika,
- o logici automatizirane obrade podataka u slučaju automatiziranog donošenja odluka.

Voditelj obrade podataka mora pružiti ispitaniku kopiju osobnih podataka koji se obrađuju. Sve informacije priopćene ispitaniku moraju se pružiti u razumljivom obliku, što znači da voditelj obrade mora osigurati da ta osoba razumije dobivene informacije. Primjerice, navođenje skraćenica iz stručnog žargona, šifriranih pojmova ili akronima u odgovoru na zahtjev za pristup obično nije dovoljan, osim ako se njihovo značenje pojasni. U slučaju automatiziranog donošenja odluka, uključujući izradu profila, potrebno je objasniti opću logiku takva postupka, uključujući kriterije koji su uzeti u obzir pri ocjenjivanju ispitanika. Unutar **prava Vijeća Europe** postoje slične odredbe⁵⁵³.

552 Opća uredba o zaštiti podataka, članak 15. stavak 1.

553 Vidjeti moderniziranu Konvenciju br. 108, članak 8. stavak 1. točku (c).

Primjer: Pristupom vlastitim osobnim podacima ispitanik može utvrditi jesu li podaci točni. Stoga je neophodno da se ispitanika na razumljiv način obavijesti ne samo o osobnim podacima koji se obrađuju već i o kategorijama u sklopu kojih se oni obrađuju, poput imena, IP adrese, geolokacijskih koordinata, broja kreditne kartice itd.

Kada podaci nisu prikupljeni od ispitanika, kao odgovor na zahtjev za pristup moraju se pružiti informacije o izvoru podatka ako su dostupne. Ta se odredba mora tumačiti u kontekstu načela poštenosti, transparentnosti i odgovornosti. Voditelj obrade ne smije uništiti informacije o izvoru podataka kako bi ih izuzeo od otkrivanja, osim ako bi se brisanje odvijalo unatoč zaprimanju zahtjeva za pristup, te se i dalje mora pridržavati općih zahtjeva „odgovornosti“.

Kako je utvrđeno sudskom praksom SEU-a, pravo na pristup osobnim podacima ne smije se nepotrebno vremenski ograničiti. Ispitanicima također treba dati razumnu mogućnost dobivanja informacija o prošlim postupcima obrade podataka.

Primjer: U predmetu *Rijkeboer*⁵⁵⁴ od SEU-a je zatraženo da utvrdi može li se pravo pojedinca na pristup informacijama o primateljima ili kategorijama primatelja osobnih podataka i o sadržaju podataka ograničiti na godinu dana prije njegova zahtjeva za pristup.

Kako bi utvrdio je li na temelju zakonodavstva EU-a dopušteno takvo vremensko ograničenje, SEU je odlučio tumačiti članak 12. u kontekstu svrha Direktive. Prvo je istaknuo da je pravo na pristup nužno kako bi ispitanik mogao ostvariti svoje pravo da voditelj obrade ispravi, izbriše ili blokira njegove podatke ili obavijesti treće strane kojima su podaci otkriveni o toj ispravci, brisanju ili blokiranju. Stvarno pravo na pristup nužno je i kako bi se ispitaniku dala mogućnost da ostvari svoje pravo na prigovor na obradu osobnih podataka ili pravo na podnošenje pritužbe i traženje odštete⁵⁵⁵.

⁵⁵⁴ SEU, C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 7. svibnja 2009.

⁵⁵⁵ Opća uredba o zaštiti podataka, članak 15. stavak 1. točke (c) i (f), članak 16., članak 17. stavak 2., članak 21. te poglavlje VIII.

Radi osiguravanja praktičnog učinka prava dodijeljenih ispitanicima, SEU je smatrao da se „to pravo mora obavezno odnositi na prošlost. U suprotnom ispitanik ne bi mogao učinkovito ostvariti svoje pravo na ispravak, brisanje ili blokiranje podataka koji se smatraju nezakonitima ili netočnima, odnosno na pokretanje sudskog postupka i naknadu za pretrpljenu štetu”.

6.1.2. Pravo na ispravak

Prema pravu EU-a i Vijeća Europe, ispitanici imaju pravo na ispravak svojih osobnih podataka. Točnost osobnih podataka ključna je za osiguranje visoke razine zaštite podataka ispitanika⁵⁵⁶.

Primjer: U predmetu *Ciubotaru protiv Moldavije*⁵⁵⁷ tužitelj nije mogao promijeniti upis svojeg etničkog podrijetla u službenoj evidenciji s moldavskog na rumunjsko, navodno zbog toga što nije potkrijepio svoj zahtjev. ESLJP je smatrao da je prihvatljivo da države zatraže objektivan dokaz pri upisu etničkog podrijetla pojedinca. Ako se takav zahtjev temelji isključivo na subjektivnim i nepotkrijepljenim temeljima, nadležna tijela mogu ga odbiti. Međutim, tužiteljev zahtjev nije bio utemeljen samo na subjektivnom poimanju vlastitog etničkog podrijetla. On je iznio svoje veze s rumunjskom etničkom skupinom koje su se mogle objektivno provjeriti, na primjer jezik, ime, empatija i drugo. Međutim, prema nacionalnom zakonodavstvu, tužitelj je morao osigurati dokaze da su njegovi roditelji pripadali rumunjskoj etničkoj skupini. S obzirom na povijesnu situaciju u Moldaviji takav je zahtjev stvorio nepremostivu prepreku upisu etničkog identiteta koji bi se razlikovao od onog upisanog za njegove roditelje koji su zabilježila sovjetska tijela. Budući da je tužitelju onemogućila pregled njegova zahtjeva u kontekstu dokaza koji se mogu objektivno provjeriti, država nije ispunila svoju pozitivnu dužnost osiguravanja učinkovitog poštovanja privatnog života tužitelja. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

U nekim je slučajevima dovoljno da ispitanik jednostavno zatraži ispravak, na primjer, pravopisne greške u imenu, promjenu adrese ili telefonskog broja. Sukladno **pravu EU-a i Vijeća Europe**, netočni osobni podaci moraju se ispraviti bez nepotrebne

⁵⁵⁶ *Ibid.*, članak 16. i uvodna izjava 65.; modernizirana Konvencija br. 108, članak 9. stavak 1. točka (e).

⁵⁵⁷ ESLJP, *Ciubotaru protiv Moldavije*, br. 27138/04, 27. travnja 2010., t. 51. i 59.

ili prekomjerne odgode⁵⁵⁸. Međutim, ako su takvi zahtjevi povezani s pravno značajnim pitanjima, kao što je pravni identitet ispitanika ili mjesto prebivališta radi dostave pravnih dokumenata, zahtjevi za ispravke možda neće biti dovoljni i voditelj obrade će moći zatražiti dokaz navodne netočnosti. Takvim se zahtjevima ispitaniku ne smije nametnuti nerazuman teret dokaza i tako onemogućiti ispravak njezinih podataka. ESLJP je utvrdio kršenja članka 8. EKLJP-a u nekoliko slučajeva u kojima tužitelj nije mogao opovrgnuti točnost informacija iz tajnih registara⁵⁵⁹.

Primjer: U predmetu *Cemalettin Canli protiv Turske*⁵⁶⁰ ESLJP je utvrdio kršenje članka 8. EKLJP-a u netočnom policijskom izvješću u kaznenom postupku.

Tužitelj je dvaput bio podvrgnut kaznenom postupku zbog navodnog članstva u nezakonitim organizacijama, no nikad nije bio osuđen. Kad je tužitelj ponovno uhićen i optužen za još jedno kazneno djelo, policija je kaznenom sudu predala izvješće pod naslovom „Obrazac s informacijama o dodatnim kaznenim djelima“, u kojemu je tužitelj naveden kao član dviju nezakonitih organizacija. Zahtjev tužitelja za izmjenu izvješća i policijske evidencije bio je neuspješan. ESLJP je smatrao da su informacije u policijskom izvješću bile u okviru članka 8. Europske konvencije o ljudskim pravima jer bi javne informacije također mogle spadati u kategoriju „privatnog života“ ako se sustavno prikupljaju i pohranjuju u datotekama koje čuvaju nadležna tijela. Osim toga, policijsko izvješće bilo je netočno sastavljeno, a njegovo podnošenje kaznenom sudu nije bilo u skladu s nacionalnim zakonom. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Tijekom građanskog postupka ili postupka pred javnim tijelom u kojem se odlučuje o točnosti podataka, ispitanik može zatražiti bilježenje naznake ili napomene o osporavanju točnosti i čekanju službene odluke u svojoj podatkovnoj datoteci⁵⁶¹. U tom razdoblju voditelj obrade podataka ne smije podatke predstavljati kao točne ili kao izuzete od izmjene, naročito trećim strankama.

558 Opća uredba o zaštiti podataka, članak 16.; modernizirana Konvencija br. 108, članak 9. stavak 1.

559 ESLJP, *Rotaru protiv Rumunjske* [VV], br. 28341/95, 4. svibnja 2000.

560 ESLJP, *Cemalettin Canli protiv Turske*, br. 22427/04, 18. studenoga 2008., t. 33., 42. i 43.; ESLJP, *Dalea protiv Francuske*, br. 964/07, 2. veljače 2010.

561 Opća uredba o zaštiti podataka, članak 18. i uvodna izjava 67.

6.1.3. Pravo na brisanje („pravo na zaborav“)

Pružanje prava ispitanicima na brisanje vlastitih podataka posebno je važno za djelotvornu primjenu načela zaštite podataka, prvenstveno načela smanjenja količine podataka (osobni podaci moraju biti ograničeni na ono što je nužno za svrhe u koje se podaci obrađuju). Pravo na brisanje stoga je utvrđeno pravnim instrumentima Vijeća Europe i Europske unije⁵⁶².

Primjer: U predmetu *Segerstedt-Wiberg i drugi protiv Švedske*⁵⁶³ tužitelji su bili povezani s određenim liberalnim i komunističkim političkim strankama. Sumnjali su na to da su informacije o njima unesene u sigurnosnu policijsku evidenciju te su zatražili njihovo brisanje. ESLJP je prihvatio činjenicu da je pohrana predmetnih podataka imala pravnu osnovu i legitimnu svrhu. Međutim, u pogledu nekih tužitelja ESLJP je utvrdio da je kontinuirano zadržavanje podataka predstavljalo nerazmjerno miješanje u njihove privatne živote. Na primjer, u slučaju jednog tužitelja nadležna su tijela zadržala informaciju da je 1969. navodno zagovarao nasilan otpor policijskoj kontroli tijekom demonstracija. ESLJP je utvrdio da te informacije nisu mogle biti ni u kakvu interesu nacionalne sigurnosti, naročito s obzirom na to da se odnose na prošlost. ESLJP je zaključio da je prekršen članak 8. Konvencije u pogledu četvorice od petorice podnositelja jer daljnje zadržavanje njihovih podataka nije bilo korisno zbog dugog razdoblja koje je proteklo od navodnih djela koja su počinili.

Primjer: U predmetu *Brunet protiv Francuske*⁵⁶⁴ tužitelj je prijavio pohranu njegovih osobnih podataka u policijskoj bazi podataka koja je sadržavala informacije o osuđenim osobama, optuženicima i žrtvama. Iako je kazneni postupak protiv tužitelja obustavljen, njegovi su podaci bili navedeni u bazi podataka. ESLJP je zaključio da je prekršen članak 8. Konvencije. Prilikom donošenja odluke ESLJP je smatrao da u praksi nije postojala mogućnost da tužitelj izbriše svoje osobne podatke iz baze podataka. ESLJP je također razmotrio prirodu informacija uvrštenih u bazu podataka i zaključio da se time narušava tužiteljeva privatnost jer su one sadržavale pojedinosti o njegovu identitetu i osobnosti. Usto, zaključio je da je razdoblje zadržavanja osobne evidencije u bazi podataka, koje je trajalo 20 godina, bilo predugo, posebice jer tužitelj nikada nije bio osuđen.

⁵⁶² *Ibid.*, članak 17.

⁵⁶³ ESLJP, *Segerstedt-Wiberg i drugi protiv Švedske*, br. 62332/00, 6. lipnja 2006., t. 89. i 90.; primjerice, vidjeti i ESLJP, *M. K. protiv Francuske*, br. 19522/09, 18. travnja 2013.

⁵⁶⁴ ESLJP, *Brunet protiv Francuske*, br. 21010/10, 18. rujna 2014.

U moderniziranoj Konvenciji br. 108 izričito se potvrđuje da svaki pojedinac ima pravo na brisanje netočnih, pogrešnih ili nezakonito obrađenih podataka⁵⁶⁵.

U okviru prava EU-a, člankom 17. OUZP-a utvrđuje se pravo ispitanika na brisanje podataka. Pravo na brisanje osobnih podataka bez nepotrebnog odgađanja primjenjuje se:

- ako osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni,
- ako ispitanik povuče privolu na kojoj se obrada temelji i ako ne postoji druga pravna osnova za obradu,
- ako ispitanik uloži prigovor na obradu te ne postoje jači legitimni razlozi za obradu,
- ako su osobni podaci nezakonito obrađeni,
- ako se osobni podaci moraju brisati radi poštovanja pravne obveze iz prava Unije ili države članice kojem podliježe voditelj obrade,
- ako su osobni podaci prikupljeni u vezi s ponudom usluga informacijskog društva djeci sukladno članku 8. OUZP-a⁵⁶⁶.

Teret dokazivanja da je obrada podataka zakonita snose voditelji obrade jer su oni odgovorni za zakonitost obrade⁵⁶⁷. Prema načelu odgovornosti, voditelj obrade mora u svakom trenutku biti u mogućnosti dokazati da postoji čvrsta pravna osnova za obradu podataka. U suprotnom se obrada mora prekinuti⁵⁶⁸. OUZP-om se definiraju izuzeća od prava na zaborav, uključujući slučajeve u kojima je obrada osobnih podataka nužna:

- radi ostvarivanja prava na slobodu izražavanja i informiranja,

565 Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (e).

566 Opća uredba o zaštiti podataka, članak 17. stavak 1.

567 *Ibid.*

568 *Ibid.*, članak 5. stavak 2.

- radi poštovanja pravne obveze kojom se zahtijeva obrada prema pravu Unije ili pravu države članice kojom podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade,
- zbog javnog interesa u području javnog zdravlja,
- u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe,
- radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva⁵⁶⁹.

SEU je potvrdio važnost prava na brisanje za osiguravanje visoke razine zaštite podataka.

Primjer: U predmetu *Google Spain*⁵⁷⁰ SEU je razmatrao je li društvo Google bilo obvezano izbrisati zastarjele informacije o financijskim poteškoćama tužitelja iz popisa rezultata pretraživanja. Među ostalim, društvo Google osporavalo je svoju odgovornost, tvrdeći da ono pruža samo poveznicu na internetsku stranicu izdavača na kojoj stoje informacije, u ovom slučaju stranicu novina koje su objavile članak o stečaju tužitelja⁵⁷¹. Google je tvrdio da se zahtjev za brisanje zastarjelih informacija s internetske stranice treba uputiti vlasniku internetske stranice, a ne društvu Google, koje samo pruža poveznicu na izvornu stranicu. SEU je zaključio da društvo Google prilikom pretraživanja informacija i internetskih stranica na internetu te indeksiranja sadržaja radi pružanja rezultata pretraživanja postaje voditelj obrade podataka na kojeg se primjenjuju odgovornosti i obveze na temelju prava Unije.

⁵⁶⁹ *Ibid.*, članak 17. stavak 3.

⁵⁷⁰ SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. od 55. do 58.

⁵⁷¹ Google je također osporio primjenu propisa EU-a o zaštiti podataka zbog činjenice da društvo Google Inc. ima poslovni nastan u SAD-u te da se predmetna obrada osobnih podataka također odvijala u SAD-u. Drugi argument protiv primjene zakonodavstva EU-a o zaštiti podataka odnosio se na tvrdnju da se internetske tražilice ne mogu smatrati „voditeljima obrade” u pogledu podataka koji se prikazuju u njihovim rezultatima jer nemaju saznanja o tim podacima niti ih kontroliraju. SEU je odbacio oba argumenta tvrdeći da je Direktiva 95/46/EZ primjenjiva u tom slučaju te je nastavio razmatrati područje primjene prava koja su njome zajamčena, a posebice prava na brisanje osobnih podataka.

SEU je pojasnio da internetske tražilice i rezultati pretraživanja koji sadrže osobne podatke mogu poslužiti za izradu detaljnog profila osobe⁵⁷². Internetske tražilice čine informacije sadržane u takvu popisu široko dostupnima. Uzimajući u obzir moguću ozbiljnost miješanja, ono se ne može opravdati samo ekonomskim interesom koji voditelj tražilice ima u takvoj obradi. Mora se nastojati postići pravedna ravnoteža između legitimnog interesa korisnika interneta za pristup informacijama i temeljnih prava ispitanika prema člancima 7. i 8. Povelje EU-a o temeljnim pravima. U društvu koje postaje sve više digitalizirano, zahtjev da osobni podaci budu točni i da ne prelaze ono što je nužno (odnosno javne informacije) ključan je za osiguravanje visoke razine zaštite podataka pojedinaca. „[N]adzornik u okviru svojih odgovornosti, nadležnosti i mogućnosti [mora] osigurati da ta aktivnost zadovoljava uvjete“ iz prava Unije kako bi utvrđena pravna jamstva mogla razviti svoj puni učinak⁵⁷³. To znači da pravo na brisanje vlastitih osobnih podataka kada je obrada zastarjela ili više nije potrebna također obuhvaća voditelje obrade koji repliciraju informacije⁵⁷⁴.

Prilikom razmatranja je li Google obavezan ukloniti poveznice povezane s tužiteljem SEU je zaključio da u određenim uvjetima pojedinci imaju pravo zatražiti brisanje svojih osobnih podataka. Na to se pravo može pozvati kada informacije o nekom pojedincu nisu točne, dostatne ili relevantne ili ih je previše za svrhe obrade podataka. SEU je potvrdio da to pravo nije apsolutno, nego se mora odvagnuti u odnosu na druga prava i interese, posebice interes šire javnosti na pristup određenim informacijama. Svaki zahtjev za brisanje mora se procijeniti pojedinačno kako bi se uspostavila ravnoteža između temeljnih prava na zaštitu osobnih podataka i privatni život ispitanika s jedne strane te legitimnih interesa svih korisnika interneta, uključujući izdavače, s druge. SEU je pružio smjernice o čimbenicima koje je potrebno razmotriti prilikom odvagivanja interesa. Priroda tih informacija posebno je važan čimbenik. Ako su informacije povezane s privatnim životom pojedinca te ne postoji javni interes za dostupnošću tih informacija, zaštita podataka i privatnost bile bi važnije od prava šire javnosti na pristup informacijama. S druge strane, ako

572 *Ibid.*, t. 36., 38., 80., 81. i 97.

573 *Ibid.*, t. od 81. do 83.

574 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. 88. Vidjeti i: Radna skupina iz članka 29. (2014.), *Smjernice o provedbi presude Suda Europske unije u predmetu „Google Spain i Inc protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González“, C-131/12, WP 225, Bruxelles, 26. studenoga 2014., i Preporuku CM/Rec 2012(3) Odbora ministara državama članicama o zaštiti ljudskih prava u pogledu internetskih tražilica, 4. travnja 2012.*

je ispitanik javna ličnost ili priroda informacija opravdava njihovo stavljanje na raspolaganje široj javnosti, prevladavajući interes šire javnosti za pristup informacijama može biti opravdanje za miješanje u temeljna prava na zaštitu podataka i privatnost ispitanika.

Slijedom te presude, Radna skupina iz članka 29. usvojila je smjernice o provedbi odluke SEU-a⁵⁷⁵. Smjernice sadrže popis uobičajenih kriterija koje nadzorna tijela mogu upotrijebiti prilikom obrade pritužbi povezanih sa zahtjevima pojedinaca za brisanje, objašnjavanja svega što pravo na brisanje podrazumijeva te vođenja osoba kroz postupak odvagivanja prava. U smjernicama se ponavlja tvrdnja da se procjene moraju provesti pojedinačno za svaki slučaj. Budući da pravo na zaborav nije apsolutno, ishod zahtjeva može se razlikovati od slučaja do slučaja. To je vidljivo i u sudskoj praksi SEU-a nakon presude u predmetu Google.

Primjer: U predmetu *Camera di Commercio di Lecce protiv Mannija*⁵⁷⁶ SEU je morao istražiti je li pojedinac imao pravo na brisanje svojih osobnih podataka objavljenih u javnom registru trgovačkih društava nakon što je njegovo trgovačko društvo prestalo postojati. G. Manni zatražio je od Gospodarske komore Grada Leccea u Italiji da izbriše njegove osobne podatke iz tog registra nakon što je otkrio da bi potencijalni klijenti pretraživali registar i saznali da je nekada bio upravitelj društva koje je proglasilo stečaj više od desetljeća ranije. Tužitelj je smatrao da bi te informacije odvratile potencijalne klijente.

Prilikom odvagivanja prava g. Mannija na zaštitu njegovih osobnih podataka s interesom šire javnosti za pristup tim informacijama, SEU je prvo razmotrio svrhu javnog registra. Istaknuo je činjenicu da je objava podataka propisana zakonom, a posebice direktivom EU-a kojoj je svrha učiniti podatke o društvima dostupnijima trećim stranama. Treće stranke tako bi ostvarile pristup i mogle proučiti osnovnu dokumentaciju i druge informacije o određenom društvu, „posebno pojedinosti o osobama koje su ovlaštene obvezati trgovačko društvo”. Svrha otkrivanja bila je također zajamčiti pravnu sigurnost

575 Radna skupina iz članka 29. (2014.), *Smjernice o provedbi presude Suda Europske unije u predmetu „Google Spain i Inc protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González”, C-131/12*, WP 225, Bruxelles, 26. studenoga 2014.

576 SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. ožujka 2017.

s obzirom na jačanje trgovine među državama članicama, osiguravajući da treće strane imaju pristup svim relevantnim informacijama o društvima u cijelom EU-u.

SEU je također napomenuo da prava i zakonske odredbe društva često nastavljaju vrijediti i nakon proteka određenog vremena te čak nakon likvidacije društva. Sporovi povezani s likvidacijom mogu se oduljiti, a pitanja o društvu, njegovim upraviteljima i stečajnim upraviteljima mogu se postaviti i godinama nakon prestanka njegova postojanja. SEU je smatrao da se, s obzirom na brojne moguće scenarije i raznolikost rokova zastare propisanih u pojedinim državama članicama, „čini [...] da je u ovom trenutku nemoguće utvrditi jedinstveni rok, koji počinje teći od prestanka društva, po čijem isteku upis navedenih podataka u registru i njihovo objavljivanje više nije potrebno“. Zbog legitimnog cilja otkrivanja podataka i poteškoća u utvrđivanju razdoblja po čijem bi se isteku osobni podaci mogli izbrisati iz registra bez ugrožavanja interesa trećih strana, SEU je zaključio da se propisima EU-a o zaštiti podataka ne jamči pravo na brisanje osobnih podataka za osobe koje se nađu u situaciji g. Mannija.

Kada voditelj obrade učini osobne podatke javno dostupnima te ih potom mora izbrisati, dužan je i mora poduzeti odgovarajuće korake kako bi obavijestio druge voditelje obrade koji obrađuju iste podatke o zahtjevu za brisanje ispitanika. Aktivnosti voditelja obrade moraju se temeljiti na dostupnim tehnologijama i troškovima provedbe⁵⁷⁷.

6.1.4. Pravo na ograničenje obrade

Člankom 18. OUZP-a ispitanicima se omogućuje da privremeno ograniče obradu svojih osobnih podataka koju provodi voditelj obrade. Ispitanici mogu od voditelja obrade zatražiti da ograniči obradu u sljedećim slučajevima:

- osporava se točnost osobnih podataka,
- obrada je nezakonita i ispitanik traži ograničenje uporabe osobnih podataka umjesto njihova brisanja,

⁵⁷⁷ Opća uredba o zaštiti podataka, članak 17. stavak 2. i uvodna izjava 66.

- podaci se moraju čuvati radi ostvarivanja ili obrane pravnih zahtjeva,
- očekuje se odluka o tome nadilaze li legitimni interesi voditelja obrade podataka interese ispitanika⁵⁷⁸.

Metode kojima voditelj obrade može ograničiti obradu osobnih podataka mogu uključivati, primjerice, privremeno premještanje odabranih osobnih podataka u drugi sustav obrade, činjenje odabranih podataka nedostupnima za korisnike ili privremeno uklanjanje osobnih podataka⁵⁷⁹. Voditelj obrade mora obavijestiti ispitanika prije nego što ograničenje obrade bude ukinuto⁵⁸⁰.

Obveza izvješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade

Voditelj obrade mora priopćiti svaki ispravak ili brisanje osobnih podataka ili ograničenje obrade svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjeran napor⁵⁸¹. Ako ispitanik zatraži informacije o tim primateljima, voditelj obrade mora mu ih pružiti⁵⁸².

6.1.5. Pravo na prenosivost podataka

Prema OUZP-u, ispitanici imaju pravo na prenosivost podataka u situacijama u kojima se osobni podaci koje pruže voditelju obrade obrađuju automatiziranim putem na temelju privole ili kada je obrada osobnih podataka nužna za izvršenje ugovora te se provodi automatiziranim putem. To znači da se pravo na prenosivost podataka ne primjenjuje u slučajevima u kojima se obrada osobnih podataka temelji na pravnoj osnovi koja nije privola ili ugovor⁵⁸³.

Ako se pravo na prenosivost podataka primjenjuje, ispitanici imaju pravo na izravan prijenos osobnih podataka od jednog voditelja obrade drugome ako je to tehnički izvedivo⁵⁸⁴. Da bi to olakšao, voditelj obrade treba razviti interoperabilne formate

⁵⁷⁸ *Ibid.*, članak 18. stavak 1.

⁵⁷⁹ *Ibid.*, uvodna izjava 67.

⁵⁸⁰ *Ibid.*, članak 18. stavak 3.

⁵⁸¹ *Ibid.*, članak 19.

⁵⁸² *Ibid.*

⁵⁸³ *Ibid.*, uvodna izjava 68. i članak 20. stavak 1.

⁵⁸⁴ *Ibid.*, članak 20. stavak 2.

kojima se ispitanicima omogućuje prenosivost podataka⁵⁸⁵. OUZP-om se utvrđuje da ti formati moraju biti strukturirani, uobičajeno upotrebljavani i strojno čitljivi kako bi se olakšala interoperabilnost⁵⁸⁶. Interoperabilnost se u širem smislu može definirati kao sposobnost informacijskih sustava da razmjenjuju podatke i omogućuju dijeljenje informacija⁵⁸⁷. Iako je svrha formata koji se rabe postizanje interoperabilnosti, u OUZP-u se ne navode konkretne preporuke u pogledu posebnih formata; oni se mogu razlikovati od sektora do sektora⁵⁸⁸.

Prema Smjernicama Radne skupine iz članka 29., pravom na prenosivost podataka „podupiru [se] korisnički izbor, kontrola i osnaživanje korisnika” kako bi ispitanici preuzeli kontrolu nad svojim osobnim podacima⁵⁸⁹. U smjernicama se opisuju glavni elementi prenosivosti podataka, koji uključuju sljedeće:

- pravo ispitanika da prime vlastite osobne podatke koje je obradio voditelj obrade u strukturiranom, uobičajeno upotrebljavanom, strojno čitljivom i interoperabilnom formatu,
- pravo prijenosa osobnih podataka od jednog voditelja obrade podataka drugom bez ometanja ako je to tehnički izvedivo,
- režim kontrole: kada voditelj obrade odgovara na zahtjev za prenosivost podataka, djeluje prema uputama ispitanika, što znači da nije odgovoran za usklađenost primatelja s pravom zaštite podataka jer ispitanik odlučuje kome se podaci prenose,
- ostvarivanje prava na prenosivost podataka bez dovođenja bilo kojeg drugog prava u pitanje, što vrijedi i za druga prava iz OUZP-a.

585 *Ibid.*, uvodna izjava 68. i članak 20. stavak 1.

586 *Ibid.*, uvodna izjava 68.

587 Europska komisija, Komunikacija „Jači i pametniji informacijski sustavi za granice i sigurnost”, COM(2016) 205 final, 2. travnja 2016.

588 Radna skupina iz članka 29. (2016.), *Smjernice o pravu na prenosivost podataka*, WP 242, 13. prosinca 2016., revidirane 5. travnja 2017., str. 17.–18.

589 *Ibid.*

6.1.6. Pravo na prigovor

Ispitanici imaju pravo uložiti prigovor na obradu osobnih podataka na temelju svoje posebne situacije te podataka koji se obrađuju za potrebe izravnog marketinga. Pravo na prigovor može se ostvariti automatiziranim putem.

Pravo na prigovor na temelju posebne situacije ispitanika

Ne postoji opće pravo ispitanika na prigovor na obradu njihovih podataka⁵⁹⁰. Članom 21. stavkom 1. OUZP-a ispitanicima se daje pravo da ulože prigovor na temelju svoje posebne situacije ako je pravna osnova obrade ispunjavanje zadaće voditelja obrade u javnom interesu ili ako se obrada temelji na legitimnim interesima voditelja obrade⁵⁹¹. Pravo na prigovor primjenjuje se na aktivnosti izrade profila. Slično pravo potvrđeno je i moderniziranom Konvencijom br. 108⁵⁹².

Cilj prava na prigovor na temelju posebne situacije ispitanika jest postići odgovarajuću ravnotežu između prava ispitanika na zaštitu podataka i legitimnih prava drugih u postupku obrade njihovih podataka. Međutim, SEU je pojasnio da prava ispitanika općenito imaju prevagu nad ekonomskim interesima voditelja obrade podataka ovisno o „naravi informacije o kojoj je riječ, o njezinoj osjetljivosti u odnosu na privatnost osobe čiji se podaci obrađuju kao i o javnom interesu za tu informaciju”⁵⁹³. Sukladno OUZP-u, teret dokazivanja snose voditelji obrade koji moraju dokazati da postoje uvjerljivi razlozi za nastavak obrade⁵⁹⁴. Jednako tako, u Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 pojašnjava se da se legitimni razlozi za obradu podataka (koji mogu prevagnuti nad pravom ispitanika na prigovor) moraju dokazivati za svaki pojedini slučaj⁵⁹⁵.

590 Vidjeti i ESLJP, *M. S. protiv Švedske*, br. 20837/92, 27. kolovoza 1997. (predmet u kojemu su medicinski podaci priopćeni bez privole ili mogućnosti prigovora); ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.; ESLJP, *Mosley protiv Ujedinjene Kraljevine*, br. 48009/08, 10. svibnja 2011.

591 Opća uredba o zaštiti podataka, uvodna izjava 69.; članak 6. stavak 1. točke (e) i (f).

592 Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (d); Preporuka o izradi profila, članak 5. stavak 3.

593 SEU, C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014., t. 81.

594 Vidjeti i moderniziranu Konvenciju br. 108, članak 98. stavak 1. točku (d), u kojoj stoji da osoba koja daje podatke može uložiti prigovor na obradu svojih podataka, „osim ako voditelj obrade dokaže legitimne razloge za obradu koji imaju prevagu nad njezinim interesima ili pravima i temeljnim slobodama”.

595 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 78.

Primjer: U predmetu *Manni*⁵⁹⁶ SEU je smatrao da zbog legitimne svrhe otkrivanja osobnih podataka u registru trgovačkih društava, a posebice potrebe za zaštitom interesa trećih strana i osiguranje pravne sigurnosti, g. Manni u načelu nije imao pravo na brisanje svojih osobnih podataka iz registra. Međutim, potvrdio je da postoji pravo na prigovor na obradu, navodeći da „se ne može isključiti mogućnost postojanja određenih situacija u kojima jaki i zakoniti razlozi u vezi s konkretnim slučajem predmetne osobe iznimno opravdavaju ograničavanje pristupa osobnim podacima koji se na nju odnose, upisanih u registar, po isteku dovoljno dugog roka [...] trećim osobama koje imaju konkretan interes za uvid u njih“.

SEU je smatrao da su nacionalni sudovi odgovorni za procjenu svakog predmeta, uzimajući u obzir sve pojedinačne relevantne okolnosti i moguće postojanje legitimnih i jakih razloga kojima bi se iznimno mogao opravdati ograničen pristup trećih strana osobnim podacima sadržanima u registrima trgovačkih društava. Međutim, obrazložio je da se u slučaju g. Mannija činjenica da je otkrivanje njegovih osobnih podataka u registru navodno utjecalo na njegove klijente sama po sebi ne može smatrati takvim zakonitim i jakim razlogom. Potencijalni klijenti g. Mannija imaju zakonit interes za pristup informacijama o stečaju njegova prijašnjeg društva.

Rezultat je uspješnog prigovora da voditelj obrade više ne može obrađivati predmetne podatke. Međutim, postupci obrade podataka ispitanika prije prigovora i dalje su zakoniti.

Pravo na prigovor na obradu podataka u svrhu izravnog marketinga

Člankom 21. stavkom 2. OUZP-a utvrđuje se posebno pravo na prigovor na uporabu osobnih podataka za potrebe izravnog marketinga, čime se dodatno pojašnjava članak 13. Direktive o privatnosti i elektroničkim komunikacijama. To je pravo utvrđeno i u moderniziranoj Konvenciji br. 108 te Preporuci o direktnom marketingu Vijeća Europe⁵⁹⁷. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 pojašnjava

⁵⁹⁶ SEU, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. ožujka 2017., t. 47. i 60.

⁵⁹⁷ Vijeće Europe, Odbor ministara (1985.), Preporuka Rec(85)20 državama članicama o zaštiti osobnih podataka koji se koriste u svrhu direktnog marketinga, 25. listopada 1985., članak 4. stavak 1.

se da prigovori na obradu podataka za potrebe izravnog marketinga trebaju dovesti do bezuvjetnog brisanja ili uklanjanja predmetnih osobnih podataka⁵⁹⁸.

Ispitanik ima pravo na prigovor na uporabu njegovih ili njezinih osobnih podataka u svrhe izravnog marketinga, bez naplate i u bilo kojem trenutku. Ispitanici moraju o tom pravu biti jasno obaviješteni, neovisno o svim drugim informacijama.

Pravo na prigovor automatiziranim putem

Kada se osobni podaci upotrebljavaju i obrađuju za usluge informacijskog društva, ispitanik može iskoristiti svoje pravo na prigovor na obradu svojih osobnih podataka automatiziranim putem.

Usluge informacijskog društva definiraju se kao svaka usluga koja se obično pruža uz naknadu, na daljinu, elektronskim sredstvima te na osobni zahtjev primatelja usluga⁵⁹⁹.

Voditelji obrade koji pružaju usluge informacijskog društva moraju uspostaviti odgovarajuće tehničke mjere i postupke kako bi osigurali da se pravo na prigovor automatiziranim putem može učinkovito ostvariti⁶⁰⁰. Primjerice, to može uključivati blokiranje kolačića na internetskim stranicama ili isključivanje funkcije praćenja pri pretraživanju interneta.

Pravo na prigovor u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe

Sukladno pravu EU-a, znanstveno istraživanje treba se tumačiti u širokom smislu, uključujući primjerice tehnološki razvoj i demonstracijske aktivnosti, temeljno istraživanje, primijenjeno istraživanje te istraživanje koje se financira iz privatnih izvora⁶⁰¹. Povijesno istraživanje također uključuje istraživanje u genealoške svrhe, imajući u vidu da se Uredba ne bi trebala primjenjivati na preminule osobe⁶⁰². Statističke svrhe znače svako prikupljanje i obradu osobnih podataka potrebnih za statistička

598 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 79.

599 Direktiva 98/34/EZ kako je izmijenjena Direktivom 98/48/EZ o utvrđivanju postupka pružanja informacija u području tehničkih normi i propisa, članak 1. stavak 2.

600 Opća uredba o zaštiti podataka, članak 21. stavak 5.

601 *Ibid.*, uvodna izjava 159.

602 *Ibid.*, uvodna izjava 160.

istraživanja ili za proizvodnju statističkih rezultata⁶⁰³. I ovdje je posebna situacija ispitanika pravna osnova za pravo na prigovor na obradu osobnih podataka u svrhe istraživanja⁶⁰⁴. Jedina je iznimka nužnost obrade za izvršavanje zadaće zbog javnog interesa. Međutim, pravo na brisanje ne primjenjuje se kada je obrada nužna (neovisno o postojanju javnog interesa) u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe⁶⁰⁵.

U OUZP-u se uspostavlja ravnoteža između zahtjeva znanstvenog, statističkog ili povijesnog istraživanja i prava ispitanika pomoću posebnih zaštitnih mjera i odstupanja iz članka 89. Stoga se pravom Unije ili države članice mogu propisati odstupanja od prava na prigovor u mjeri u kojoj je vjerojatno da bi takvo pravo onemogućilo ili znatno ugrozilo ispunjenje istraživačkih svrha, ako su takva odstupanja nužna za ispunjenje tih svrha.

Unutar **prava Vijeća Europe** člankom 9. stavkom 2. modernizirane Konvencije br. 108 utvrđuje se da se ograničenja prava ispitanika, uključujući pravo na prigovor, mogu propisati zakonom o obradi podataka u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe ako ne postoji jasan rizik kršenja prava i temeljnih sloboda ispitanika.

Međutim, u Izvješću s objašnjenjima (stavak 41.) također se utvrđuje da ispitanici trebaju imati mogućnost dati privolu samo za određena područja istraživanja ili dijelove istraživačkih projekata u mjeri u kojoj to predviđena svrha dopušta te uložiti prigovor ako smatraju da se obradom prekomjerno narušavaju njihova prava i slobode bez legitimne osnove.

Drugim riječima, takva bi se obrada unaprijed smatrala usklađenom pod uvjetom da postoje druge zaštitne mjere i da se u tim postupcima u načelu izuzima svaka uporaba informacija prikupljenih za donošenje odluka ili mjera o određenom pojedincu.

603 *Ibid.*, uvodna izjava 162.

604 *Ibid.*, članak 21. stavak 6.

605 *Ibid.*, članak 17. stavak 3. točka (d).

6.1.7. Automatizirano pojedinačno donošenje odluka, uključujući izradu profila

Automatizirane odluke jesu odluke donesene na temelju osobnih podataka obrađenih isključivo automatiziranim putem, bez ljudske intervencije. **Prema pravu EU-a**, ispitanici ne smiju biti podvrgnuti automatiziranim odlukama koje imaju pravni ili sličan učinak. Ako je za takve odluke vjerojatno da će znatno utjecati na živote pojedinaca jer se odnose, na primjer, na kreditnu sposobnost, zapošljavanje putem interneta, učinak na poslu ili analizu ponašanja ili pouzdanosti, nužna je posebna zaštita radi izbjegavanja negativnih posljedica. Automatizirano donošenje odluka uključuje izradu profila koja se sastoji od svakog oblika automatske procjene „osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca”⁶⁰⁶.

Primjer: Radi brze ocjene kreditne sposobnosti budućeg klijenta, agencije za kreditni rejting (CRA) prikupljaju određene podatke, kao što su način na koji je klijent održavao svoj kreditni račun i uslužne/komunalne račune, pojedinih o njegovim prethodnim adresama te informacije iz javnih izvora poput popisa birača, javnih evidencija (uključujući sudske presude) ili podataka o bankrotu ili insolventnosti. Ti se osobni podaci potom učitavaju u algoritam za ocjenjivanje koji izračunava ukupnu vrijednost koja predstavlja kreditnu sposobnost potencijalnog klijenta.

Prema Radnoj skupini iz članka 29., pravo da se na pojedinca ne odnose odluke koje se temelje isključivo na automatiziranoj obradi koje mogu proizvesti pravne učinke za ispitanika ili koje znatno na njega utječu jednako je općoj zabrani i ne zahtijeva da ispitanik proaktivno uloži prigovor na takvu odluku⁶⁰⁷.

Ipak, sukladno OUZP-u, automatizirano donošenje odluka koje proizvode pravne učinke ili značajno utječu na pojedince može biti prihvatljivo ako je nužno za sklapanje ili izvršenje ugovora između voditelja obrade podataka i ispitanika ili ako ispitanik da izričitu privolu. Automatizirano donošenje odluka također je prihvatljivo ako je

⁶⁰⁶ *Ibid.*, uvodna izjava 71., članak 4. stavak 4. i članak 22.

⁶⁰⁷ Radna skupina iz članka 29., *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. listopada 2017., str. 15.

dopušteno zakonom te ako su prava, slobode i legitimni interesi ispitanika odgovarajuće zaštićeni⁶⁰⁸.

Među obvezama voditelja obrade u vezi s informacijama koje treba pružiti prilikom prikupljanja osobnih podataka, OUZP-om se propisuje i da ispitanici moraju biti obaviješteni o postojanju automatiziranog donošenja odluka, uključujući izradu profila⁶⁰⁹. To ne utječe na pravo na pristup osobnim podacima koje obrađuje voditelj obrade⁶¹⁰. Informacije ne bi trebale upućivati samo na činjenicu da će se izraditi profil već bi trebale sadržavati i smislene informacije o logici na kojoj se izrada profila temelji te predviđenim posljedicama takve obrade za pojedince⁶¹¹. Primjerice, društvo za zdravstveno osiguranje koje upotrebljava automatizirano donošenje odluka o zahtjevima treba ispitanicima pružiti opće informacije o načinu rada algoritma i faktorima s pomoću kojih algoritam izračunava njihove premije osiguranja. Jednako tako, prilikom ostvarivanja „prava na pristup” ispitanici mogu zatražiti informacije od voditelja obrade o postojanju automatiziranog donošenja odluka i smislene informacije o tome o kojoj je logici riječ⁶¹².

Svrha informacija pruženih ispitanicima jest osigurati transparentnost i omogućiti ispitanicima da daju privolu utemeljenu na informacijama, ako je potrebna, ili da ostvare pravo na ljudsku intervenciju. Voditelj obrade podataka mora provesti odgovarajuće mjere za zaštitu prava, sloboda i legitimnih interesa ispitanika. To uključuje barem pravo na ljudsku intervenciju voditelja obrade te mogućnost da ispitanik izrazi vlastito stajalište i ospori odluku na temelju automatizirane obrade svojih osobnih podataka⁶¹³.

Radna skupina iz članka 29. izradila je dodatne smjernice o uporabi automatiziranog donošenja odluka na temelju OUZP-a⁶¹⁴.

Prema pravu Vijeća Europe, pojedinci imaju pravo na to da se o njima ne donose odluke koje značajno utječu na njih ili koje se temelje isključivo na automatiziranoj

608 Opća uredba o zaštiti podataka, članak 22. stavak 2.

609 *Ibid.*, članak 12.

610 *Ibid.*, članak 15.

611 *Ibid.*, članak 13. stavak 2. točka (f).

612 *Ibid.*, članak 15. stavak 1. točka (h).

613 *Ibid.*, članak 22. stavak 3.

614 Radna skupina iz članka 29. (2017.), *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. listopada 2017.

obradi bez uzimanja u obzir njegova mišljenja⁶¹⁵. Zahtjev za uzimanje u obzir mišljenja ispitanika kada se odluke temelje isključivo na automatiziranoj obradi podrazumijeva da osoba ima pravo osporiti takve odluke te da bi trebala imati mogućnost osporiti svaku netočnost osobnih podataka koje voditelj obrade upotrebljava i relevantnost bilo kojeg profila koji se na nju primjenjuje⁶¹⁶. Međutim, pojedinac ne može ostvariti to pravo ako je automatizirana odluka dozvoljena zakonom kojemu voditelj obrade podliježe i kojim se uspostavljaju odgovarajuće mjere za zaštitu prava, sloboda i legitimnih interesa ispitanika. Usto, ispitanici imaju pravo na zahtjev dobiti informacije o razlozima za obradu podataka koja se provodi⁶¹⁷. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se primjer određivanja kreditne sposobnosti. Pojedinci bi trebali imati pravo saznati ne samo za pozitivnu ili negativnu odluku o kreditnoj sposobnosti nego i za *logiku* na kojoj se temelji obrada njihovih osobnih podataka koja je dovela do takve odluke. „Razumijevanje tih elemenata doprinosi djelotvornoj provedbi drugih ključnih zaštitnih mjera, poput prava na prigovor i prava na pritužbu nadležnom tijelu”⁶¹⁸.

Iako nije pravno obvezujuća, u Preporuci o profiliranju utvrđuju se uvjeti prikupljanja i obrade osobnih podataka u kontekstu izrade profila⁶¹⁹. Ona sadržava odredbe o potrebi da se osigura da je obrada u kontekstu izrade profila poštena, zakonita, razmjerna i služi utvrđenim i legitimnim svrhama. Također sadržava odredbe o informacijama koje voditelji obrade trebaju pružiti ispitanicima. U Preporuci je utvrđeno i načelo kvalitete podataka, prema kojem voditelji obrade moraju poduzeti mjere za ispravljanje čimbenika netočnosti podataka, ograničiti rizike ili pogreške koje izrada profila može uzrokovati te redovito ocjenjivati kvalitetu podataka i algoritama koji se upotrebljavaju.

615 Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (a).

616 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 75.

617 Modernizirana Konvencija br. 108, članak 9. stavak 1. točka (c).

618 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 77.

619 Vijeće Europe, *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling* (Preporuka CM/Rec(2010)13 Odbora ministara državama članicama o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu izrade profila), članak 5. točka (5).

6.2. Pravni lijekovi, odgovornost, kazne i naknada

Ključne točke

- Sukladno moderniziranoj Konvenciji br. 108, u nacionalnom zakonodavstvu ugovornih stranaka moraju se propisati odgovarajući pravni lijekovi i sankcije za kršenje prava na zaštitu podataka.
- OUZP-om se na razini EU-a utvrđuju pravni lijekovi za ispitanike u slučajevima kršenja njihovih prava, kao i sankcije protiv voditelja obrade i izvršitelja obrade koji se ne pridržavaju odredbi Uredbe. Njome se također utvrđuje pravo na naknadu štete i odgovornost.
- Ispitanici imaju pravo na podnošenje pritužbe nadzornom tijelu zbog navodnih kršenja Uredbe, kao i pravo na učinkovit pravni lijek i dobivanje naknade štete.
- Pri ostvarivanju prava na učinkovit pravni lijek pojedince mogu zastupati neprofitne organizacije koje djeluju u području zaštite podataka.
- Voditelj obrade ili izvršitelj obrade odgovoran je za svu materijalnu i nematerijalnu štetu koja nastane zbog kršenja prava.
- Nadzorna tijela imaju ovlast izricanja upravnih novčanih kazni za kršenja Uredbe u iznosu do 20 000 000 € ili, u slučaju poduzeća, 4 % od ukupnog godišnjeg prometa na svjetskoj razini, ovisno o tome što je veće.
- Ispitanici mogu podnijeti prijave o kršenju zakonodavstva o zaštiti podataka ESLJP-u, no samo u krajnjoj nuždi i pod određenim uvjetima.
- Svaka fizička ili pravna osoba ima pravo na podnošenje pritužbe na bilo koju odluku Europskog odbora za zaštitu podataka pred SEU-om pod uvjetima utvrđenima u Ugovorima.

Donošenje pravnih instrumenata nije dovoljno za osiguravanje zaštite osobnih podataka u Europi. Da bi europski propisi o zaštiti podataka bili učinkoviti, potrebno je uspostaviti mehanizme kojima se pojedincima omogućuje da se suprotstave kršenju svojih prava i da zatraže naknadu za bilo koju pretrpljenu štetu. Također je važno da nadzorna tijela imaju ovlast izricanja sankcija koje su učinkovite, odvraćajuće i proporcionalne prekršaju.

Prava na temelju zakonodavstva o zaštiti podataka može ostvariti osoba čija su prava dovedena u pitanje, odnosno ispitanik. Međutim, druge osobe koje ispunjavaju

odgovarajuće zahtjeve na temelju nacionalnog zakonodavstva također mogu zastupati ispitanike u postupku ostvarivanja njihova prava. Sukladno brojnim nacionalnim zakonima, djecu i osobe s intelektualnim teškoćama moraju zastupati njihovi skrbnici⁶²⁰. Prema zakonodavstvu EU-a o zaštiti podataka, udruženje čiji je zakonit cilj promicanje prava na zaštitu podataka može zastupati ispitanike pred nadzornim tijelom ili sudom⁶²¹.

6.2.1. Pravo na podnošenje pritužbe nadzornom tijelu

Prema pravu Vijeća Europe i EU-a, pojedinci imaju pravo podnijeti zahtjeve i pritužbe nadležnom nadzornom tijelu ako smatraju da se obrada njihovih osobnih podataka ne provodi u skladu sa zakonom.

U moderniziranoj Konvenciji br. 108 potvrđuje se pravo ispitanika na pomoć nadzornog tijela u ostvarivanju njihovih prava na temelju Konvencije, neovisno o njihovu državljanstvu ili prebivalištu⁶²². Zahtjev za pomoć može se odbiti samo u iznimnim okolnostima i ispitanici ne bi trebali snositi troškove i naknade povezane s tom pomoći⁶²³.

Slične se odredbe mogu pronaći i u pravnom sustavu EU-a. OUZP-om se propisuje da nadzorna tijela donesu mjere kojima će olakšati podnošenje pritužbi, poput izrade obrasca za podnošenje pritužbe elektroničkim putem⁶²⁴. Ispitanik može podnijeti pritužbu nadzornom tijelu u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mjesto ili mjesto navodnog kršenja⁶²⁵. Pritužbe se moraju istražiti, a nadzorno tijelo mora obavijestiti dotičnu osobu o ishodu postupka obrade pritužbe⁶²⁶.

620 FRA (2015.), *Piručnik o pravima djeteta u europskom pravu*, Luxembourg, Ured za publikacije Europske unije; FRA (2013.), *Legal capacity of persons with intellectual disabilities and persons with mental health problems* (Poslovna sposobnost osoba s intelektualnim teškoćama i osoba s mentalnim problemima), Luxembourg, Ured za publikacije Europske unije.

621 Opća uredba o zaštiti podataka, članak 80.

622 Modernizirana Konvencija br. 108, članak 18.

623 *Ibid.*, članci 16. i 17.

624 Opća uredba o zaštiti podataka, članak 57. stavak 2.

625 *Ibid.*, članak 77. stavak 1.

626 *Ibid.*, članak 77. stavak 2.

Potencijalna kršenja propisa u institucijama i tijelima EU-a mogu se prijaviti Europskom nadzorniku za zaštitu podataka (EDPS)⁶²⁷. Ako Europski nadzornik za zaštitu podataka ne odgovori u roku od šest mjeseci, smatra se da je pritužba odbijena. Žalbe protiv odluka EDPS-a mogu se podnijeti SEU-u u okviru Uredbe (EZ) br. 45/2001 kojom se institucijama i tijelima EU-a propisuje obveza poštovanja pravila zaštite podataka.

Mora postojati mogućnost podnošenja žalbe sudovima protiv odluka nacionalnog nadzornog tijela. To se odnosi na ispitanika kao i na voditelje obrade koji su sudjelovali u postupku pred nadzornim tijelom.

Primjer: U rujnu 2017. španjolsko nadležno tijelo za zaštitu podataka novčano je kaznilo Facebook zbog kršenja nekoliko propisa o zaštiti podataka. Nadzorno tijelo osudilo je tu društvenu mrežu zbog prikupljanja, pohranjivanja i obrade osobnih podataka u oglašivačke svrhe, uključujući posebne kategorije osobnih podataka, bez ishođenja privole ispitanika. Odluka je donesena na temelju istrage koju je nadzorno tijelo provelo na vlastitu inicijativu.

6.2.2. Pravo na učinkovit pravni lijek

Uz pravo na podnošenje pritužbe nadzornom tijelu, pojedinci moraju imati pravo na učinkovit pravni lijek i pokretanja sudskog postupka. Pravo na pravni lijek dobro je zaštićeno u europskoj pravnoj tradiciji te je prepoznato kao temeljno pravo i člankom 47. Povelje EU-a o temeljnim pravima i člankom 13. EKLP-a⁶²⁸.

Unutar prava EU-a, važnost stavljanja učinkovitog pravnog lijeka na raspolaganje ispitanicima u slučaju kršenja njihovih prava jasna je iz odredbi OUZP-a, kojima se utvrđuje pravo na učinkovit pravni lijek protiv nadzornih tijela, voditelja obrade i izvršitelja obrade, te iz sudske prakse Suda EU-a.

627 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

628 Vidjeti primjerice ESLJP, *Karabeyoğlu protiv Turske*, br. 30083/10, 7. lipnja 2016.; ESLJP, *Mustafa Sezgin Tanrıkulu protiv Turske*, br. 27473/06, 18. srpnja 2017.

Primjer: U predmetu *Schrems*⁶²⁹ SEU je Odluku o primjerenosti sigurne luke proglasio nevaljanom. Tom su odlukom bili dopušteni međunarodni prijenosi podataka iz EU-a organizacijama u SAD-u koje vrše vlastito potvrđivanje u sklopu sustava sigurne luke. SEU je smatrao da sustav sigurne luke ima nekoliko nedostataka zbog kojih se ugrožavaju temeljna prava građana EU-a na zaštitu privatnosti, zaštitu osobnih podataka i pravo na učinkovit pravni lijek.

U pogledu kršenja prava na privatnost i zaštitu podataka, SEU je istaknuo da se zakonima SAD-a određenim tijelima javne vlasti dopušta pristup osobnim podacima koji su preneseni iz država članica u SAD i njihova obrada na način koji nije u skladu sa svrhama zbog kojih su izvorno preneseni i koji prekoračuje ono što je strogo nužno i proporcionalno za nacionalnu sigurnost. U pogledu prava na učinkovit pravni lijek, napomenuo je da ispitanici nemaju mogućnost pristupa i po potrebi ispravljanja ili brisanja podataka o sebi upravnim ili sudskim putem. SEU je zaključio da propis koji ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima, ili radi ispravka ili brisanja takvih podataka, „ne poštuje bitan sadržaj temeljnog prava na djelotvornu sudsku zaštitu, kao što je to propisano u članku 47. Povelje“. Naglasio je da je postojanje pravnog lijeka kojim se osigurava poštovanje pravnih odredaba svojstveno postojanju pravne države.

Pojedinci, voditelji obrade ili izvršitelji obrade koji žele osporiti pravno obvezujuću odluku nadzornog tijela mogu pokrenuti postupak pred sudom⁶³⁰. Pojam „odluka“ treba se tumačiti u širem smislu, tako da obuhvaća provedbu istražnih, sankcijskih i autorizacijskih ovlasti nadzornog tijela te odluke o odbacivanju ili odbijanju pritužbe. Međutim, mjere koje nisu pravno obvezujuće, poput mišljenja ili savjeta koje je dalo nadzorno tijelo, ne mogu biti predmet sudskog postupka⁶³¹. Postupci protiv nadzornog tijela moraju se voditi pred sudovima države članice u kojoj ono ima poslovni nastan⁶³².

U slučajevima u kojima voditelj ili izvršitelj obrade prekrši prava ispitanika, ispitanik ima pravo podnijeti pritužbu sudu⁶³³. U postupcima pokrenutima protiv vodi-

629 SEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VW], 6. listopada 2015.

630 Opća uredba o zaštiti podataka, članak 78.

631 *Ibid.*, uvodna izjava 143.

632 *Ibid.*, članak 78. stavak 3.

633 *Ibid.*, članak 79.

telja ili izvršitelja obrade posebno je važno da pojedinci imaju mogućnost odabira mjesta pokretanja postupka. Mogu ih voditi u državi članici u kojoj voditelj ili izvršitelj obrade ima poslovni nastan ili u državi članici u kojoj dotični ispitanik ima uobičajeno boravište⁶³⁴. Druga mogućnost olakšava pojedincima da ostvare svoja prava jer im omogućuje pokretanje postupka u državi u kojoj borave i u sudskoj nadležnosti koju poznaju. Ograničavanjem mjesta za pokretanje postupaka protiv voditelja obrade i izvršitelja obrade na državu članicu u kojoj oni imaju poslovni nastan moglo bi se odvratiti ispitanike od pokretanja sudskih postupaka ako žive u drugim državama članicama jer bi to uključivalo putovanje i dodatne troškove, dok bi se sam postupak mogao voditi na stranom jeziku i u nepoznatoj nadležnosti. Jedina su iznimka predmeti u kojima je voditelj ili izvršitelj obrade javno tijelo, a postupak se vodi u sklopu izvršavanja njihovih javnih ovlasti. U tom su slučaju za predmet nadležni samo sudovi države u kojoj se nalazi dotično javno tijelo⁶³⁵.

U većini slučajeva predmeti koji se odnose na propise o zaštiti podataka rješavat će se pred sudovima država članica, no neki se predmeti mogu voditi i pred SEU-om. Prva se mogućnost odnosi na slučaj u kojem ispitanik, voditelj obrade, izvršitelj obrade ili nadzorno tijelo pokreće postupak za poništenje odluke EOZP-a. Međutim, budući da takav postupak podliježe uvjetima iz članka 263. UFEU-a, da bi bio valjan, ti pojedinci i subjekti moraju dokazati da se odluka Odbora izravno i osobno odnosi na njih.

Drugi se scenarij odnosi na slučajeve u kojima institucije i tijela EU-a nezakonito obrađuju osobne podatke. U slučajevima u kojima institucije Europske unije krše zakonodavstvo o zaštiti podataka, ispitanici mogu podnijeti tužbu Općem sudu Europske unije (Opći sud dio je SEU-a). Opći sud odgovoran je za donošenje prvostupanjskih odluka o pritužbama na kršenje prava Unije u institucijama EU-a. Stoga se pritužbe protiv EDPS-a, koji je institucija EU-a, također mogu podnijeti Općem sudu⁶³⁶.

Primjer: U predmetu *Bavarian Lager*⁶³⁷ to je društvo od Europske komisije zatražilo pristup cjelokupnom zapisniku sa sastanka koji je održala Komisija, a koji se navodno odnosio na pravna pitanja bitna za društvo. Komisija je

634 *Ibid.*, članak 79. stavak 2.

635 *Ibid.*

636 Uredba (EZ) br. 45/2001, članak 32. stavak 3.

637 SEU, C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd* [VV], 29. lipnja 2010.

odbila zahtjev društva iz razloga prevladavajućih interesa zaštite podataka⁶³⁸. Pozivajući se na članak 32. Uredbe o zaštiti podataka u institucijama Europske unije, društvo Bavarian Lager protiv te je odluke uložilo žalbu Prvostupanjskom sudu (prethodniku Općeg suda). U svojoj odluci (predmet T-194/04, *The Bavarian Lager Co. Ltd protiv Komisije Europskih zajednica*) Prvostupanjski sud poništio je odluku Komisije kojom je odbijen zahtjev za pristup. Europska komisija žalila se na tu odluku SEU-u.

Veliko vijeće SEU-a donijelo je presudu kojom je odbačena presuda Prvostupanjskog suda i potvrđeno Komisijino odbacivanje zahtjeva za pristup cjelokupnom zapisniku sa sastanka radi zaštite osobnih podataka osoba koje su prisustvovala sastanku. SEU je smatrao da Komisija nije smjela otkriti te podatke jer sudionici sastanka nisu dali privolu za otkrivanje svojih osobnih podataka. Usto, društvo Bavarian Lager nije dokazalo da mu je nužan pristup tim informacijama.

Tijekom odvijanja domaćeg postupka, ispitanici, nadzorna tijela, voditelji obrade ili izvršitelji obrade mogu od nacionalnog suda zatražiti da zahtijeva objašnjenje od Suda EU-a o tumačenju i valjanosti akata institucija, tijela, ureda ili agencija Europske unije. Takva se objašnjenja nazivaju prethodnim odlukama. To nije izravni lijek za podnositelja, ali nacionalnim sudovima omogućuje primjenu točnog tumačenja prava Unije. Upravo putem tog mehanizma prethodnih odluka ključni predmeti za razvoj zakonodavstva EU-a o zaštiti podataka došli su do SEU-u, na primjer predmeti *Digital Rights Ireland* i *Kärntner Landesregierung i dr.*⁶³⁹ te *Schrems*⁶⁴⁰.

Primjer: *Digital Rights Ireland* i *Kärntner Landesregierung i drugi*⁶⁴¹ spojeni je predmet koji su podnijeli irski Visoki sud (High Court) i austrijski Ustavni sud u vezi s usklađenošću Direktive 2006/24/EZ (Direktive o zadržavanju podataka) sa zakonodavstvom EU-a o zaštiti podataka. Austrijski Ustavni

638 Detaljna analiza rasprave dostupna je u publikaciji EDPS (2011.), *Public access to documents containing personal data after the Bavarian Lager ruling* (Javni pristup dokumentima koji sadrže osobne podatke nakon presude u predmetu Bavarian Lager), Bruxelles, EDPS.

639 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014.

640 SEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VW], 6. listopada 2015.

641 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014.

sud SEU-u je podnio pitanja u vezi s valjanošću članaka od 3. do 9. Direktive 2006/24/EZ u svjetlu članka 7., 9. i 11. Povelje EU-a o temeljnim pravima. Pitanja su se odnosila na to jesu li određene odredbe austrijskog Saveznog zakona o telekomunikacijama kojima se prenosi Direktiva o zadržavanju podataka neusklađene s aspektima nekadašnje Direktive o zaštiti podataka i Uredbe o zaštiti podataka u institucijama Europske unije.

U predmetu *Kärntner Landesregierung i dr. g. Seitlinger*, jedan od tužitelja u postupku pred Ustavnim sudom, tvrdio je da telefon, internet i e-poštu upotrebljava i u poslovne i u privatne svrhe. Sukladno tome, informacije koje je slao i primao prolazile su kroz javne telekomunikacijske mreže. Prema austrijskom Zakonu o telekomunikacijama iz 2003., njegov pružatelj telekomunikacijskih usluga bio je zakonski obavezan prikupljati i pohranjivati podatke o njegovoj uporabi mreže. G. Seitlinger smatrao je da takvo prikupljanje i pohranjivanje njegovih osobnih podataka nije bilo nužno u tehničke svrhe slanja i primanja informacija putem mreže. Osim toga, prikupljanje i pohrana tih podataka nisu nikako bili nužni u svrhu naplate. G. Seitlinger izjavio je da nije pristao na takvu uporabu svojih osobnih podataka, koji su prikupljeni i pohranjeni isključivo zbog austrijskog Zakona o telekomunikacijama iz 2003.

Stoga je g. Seitlinger pred austrijskim Ustavnim sudom pokrenuo postupak u kojem je tvrdio da se zakonskim obvezama njegova pružatelja telekomunikacijskih usluga krše njegova temeljna prava prema članku 8. Povelje EU-a o temeljnim pravima. Budući da je u austrijskom zakonodavstvu provedeno pravo Unije (tadašnja Direktiva o zadržavanju podataka), austrijski Ustavni sud prosljedio je predmet SEU-u kako bi on donio odluku o sukladnosti Direktive s pravima na privatnost i zaštitu podataka zaštićenima Poveljom EU-a o temeljnim pravima.

Veliko vijeće SEU-a donijelo je odluku o predmetu, koja je dovela do poništavanja Direktive EU-a o zadržavanju podataka. SEU je utvrdio da je Direktiva uključivala posebno ozbiljno miješanje u temeljna prava na privatnost i zaštitu podataka, koje nije bilo ograničeno na ono što je strogo nužno. Direktiva je imala legitiman cilj jer su njome nacionalnim tijelima pružene dodatne mogućnosti za istragu i progon teških kaznenih djela te je stoga bila koristan alat za kaznene istrage. Međutim, SEU je napomenuo da se ograničenja temeljnih prava trebaju primjenjivati samo ako su strogo nužna te da trebaju biti popraćena jasnim i preciznim pravilima o njihovu području primjene, zajedno sa zaštitnim mjerama za pojedince.

Prema mišljenju SEU-a, Direktiva nije ispunjavala taj kriterij nužnosti. Za početak, njome nisu utvrđena jasna i precizna pravila kojima se ograničava opseg miješanja. Umjesto postavljanja zahtjeva za povezanost zadržanih podataka s teškim kaznenim djelima, Direktiva se primjenjivala na sve metapodatke svih korisnika svih elektroničkih komunikacijskih sredstava. Stoga je predstavljala miješanje u prava na privatnost i zaštitu podataka gotovo cijele populacije EU-a, što se može smatrati nerazmjernim. Nije sadržavala uvjete za ograničenje broja osoba koje su ovlaštene za pristup osobnim podacima niti je takav pristup podlijegao postupovnim uvjetima kao što je zahtjev za odobrenje upravnog tijela ili suda prije samog pristupa. Naposljetku, Direktivom nisu utvrđene jasne zaštitne mjere za zaštitu zadržanih podataka. Stoga njome nije omogućena učinkovita zaštita podataka od rizika zlorabe, kao ni od svih nezakonitih pristupa ili korištenja tih podataka⁶⁴².

SEU u načelu mora odgovoriti na postavljena pitanja i ne može odbiti donošenje prethodne odluke jer taj odgovor ne bi bio ni relevantan ni pravovremen u pogledu izvornog predmeta. Međutim, može odbiti donošenje prethodne odluke ako pitanje nije unutar njegova područja nadležnosti⁶⁴³. SEU donosi odluku samo o sastavnim elementima upućenog zahtjeva za prethodnu odluku, a nacionalni sud zadržava nadležnost u odlučivanju u izvornom predmetu⁶⁴⁴.

Prema pravu Vijeća Europe ugovorne stranke moraju uspostaviti odgovarajuće pravosudne i nepravosudne pravne lijekove za kršenja odredbi modernizirane Konvencije br. 108⁶⁴⁵. Pritužbe na navodna kršenja prava na zaštitu podataka iz članka 8. EKLP-a koje počini ugovorna stranka EKLP-a mogu se dodatno podnijeti Europskom sudu za ljudska prava nakon što se iscrpe svi dostupni domaći pravni lijekovi. Da bi se pritužba zbog kršenja članka 8. EKLP-a podnijela ESLJP-u trebaju biti ispunjeni i drugi kriteriji prihvatljivosti (članci 34. i 35. EKLP-a)⁶⁴⁶.

642 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. travnja 2014., t. 69.

643 SEU, C-244/80, *Pasquale Foglia protiv Mariella Novello (br. 2)*, 16. prosinca 1981.; SEU, C-467/04, *Kazneni postupak protiv Giuseppe Francesco Gasparini i dr.*, 28. rujna 2006.

644 SEU, C-438/05, *International Transport Workers' Federation i Finnish Seamen's Union protiv Viking Line ABP i OÜ Viking Line Eesti* [VV], 11. prosinca 2007., t. 85.

645 Modernizirana Konvencija br. 108, članak 12.

646 EKLP, članci od 34. do 37.

Iako zahtjevi ESLJP-u mogu biti usmjereni samo protiv ugovornih stranaka, neizravno se mogu baviti i postupcima ili propustima privatnih stranaka, pod uvjetom da ugovorna stranka nije ispunila svoje pozitivne obveze prema EKLJP-u niti je osigurala dovoljnu zaštitu protiv kršenja prava na zaštitu podataka u svojem nacionalnom zakonodavstvu.

Primjer: U predmetu *K. U. protiv Finske*⁶⁴⁷ tužitelj, maloljetnik, žalio se da je o njemu objavljen oglas seksualne prirode na internetskoj stranici za upoznavanje. Pružatelj usluge nije otkrio identitet osobe koja je objavila informacije zbog obveza povjerljivosti prema finskom zakonodavstvu. Tužitelj je tvrdio da finskim zakonodavstvom nije osigurana dostatna zaštita od takvih radnji privatne osobe koja je na internetu objavila inkriminirajuće podatke o njemu. ESLJP je smatrao da su države dužne suzdržati se od proizvoljnog miješanja u privatne živote pojedinaca i da mogu podlijevati pozitivnim obvezama koje uključuju „donošenje mjera za osiguranje poštovanja privatnog života, čak i u okviru međusobnih odnosa pojedinaca”. U tužiteljevu slučaju njegova praktična i djelotvorna zaštita zahtijevala je poduzimanje učinkovitih koraka za identifikaciju i progon počinitelja. Međutim, država nije osigurala takvu zaštitu, stoga je ESLJP zaključio da je došlo do kršenja članka 8. Konvencije.

Primjer: U predmetu *Köpke protiv Njemačke*⁶⁴⁸ tužiteljica je osumnjičena za krađu na radnom mjestu te je podvrgnuta tajnom videonadzoru. ESLJP je zaključio da „ništa ne upućuje na to da domaća nadležna tijela nisu uspostavila poštenu ravnotežu, prema vlastitoj procjeni, između prava tužiteljice na poštovanje njezina privatnog života prema članku 8. i interesa njezina poslodavca da zaštiti svoja vlasnička prava i javnog interesa za ispravnom primjenom pravde”. Stoga je zahtjev proglašen neprihvatljivim.

Ako ESLJP utvrdi da je država koja je ugovorna stranka prekršila bilo koja prava koja se štite Europskom konvencijom o ljudskim pravima, ta ugovorna stranka mora izvršiti presudu ESLJP-a (članak 46. Konvencije). Izvršnim mjerama treba prvo zaustaviti kršenje i ispraviti, koliko je to moguće, negativne posljedice kršenja za tužitelja. Izvršenje presuda može iziskivati i opće mjere kojima se sprečavaju kršenja slična onima koje je utvrdio ESLJP, bilo unosom promjena u zakonodavstvo, sudsku praksu ili na drugi način.

647 ESLJP, *K. U. protiv Finske*, br. 2872/02, 2. prosinca 2008.

648 ESLJP, *Köpke protiv Njemačke* (odl.), br. 420/07, 5. listopada 2010.

Ako ESLJP utvrdi kršenje Europske konvencije o ljudskim pravima, njezinim članom 41. propisano je da taj sud može tužitelju dosuditi „pravednu naknadu” o trošku ugovorne stranke.

Pravo na ovlaštenje neprofitnog tijela, organizacije ili udruženja

OUZP-om se pojedincima koji podnose pritužbu nadzornom tijelu ili pokreću sudski postupak omogućuje da ovlaste neprofitno tijelo, organizaciju ili udruženje da ih zastupa⁶⁴⁹. Ta neprofitna tijela moraju imati ciljeve od javnog interesa u svojem statutu i biti aktivna u području zaštite podataka. Ona mogu podnositi pritužbe ili ostvarivati pravo na pravni lijek u ime ispitanika. Uredbom se državama članicama pruža mogućnost da sukladno svojem nacionalnom zakonodavstvu odluče može li takvo tijelo podnositi pritužbe u ime ispitanika bez njihova posebnog ovlaštenja za to.

To pravo zastupanja omogućuje pojedincima da iskoriste stručna znanja i organizacijske i financijske resurse takvih neprofitnih tijela te tako lakše ostvare svoja prava. OUZP-om se omogućuje da takva tijela podnose kolektivne zahtjeve u ime više ispitanika. Time se doprinosi funkcioniranju i učinkovitosti pravosudnog sustava jer se slični zahtjevi okupljaju i zajednički razmatraju.

6.2.3. Odgovornost i pravo na naknadu štete

Pravom na učinkovit pravni lijek pojedincima se mora pružiti mogućnost da zatraže naknadu za bilo kakvu štetu koju pretrpe zbog obrade njihovih osobnih podataka na način kojim se krši mjerodavno zakonodavstvo. Odgovornost voditelja obrade i izvršitelja obrade za nezakonitu obradu izričito se spominje u OUZP-u⁶⁵⁰. Uredbom se pojedincima dodjeljuje pravo na naknadu štete od voditelja obrade ili izvršitelja obrade za materijalnu i nematerijalnu štetu, dok se u uvodnim izjavama utvrđuje sljedeće: „pojam štete trebalo bi široko tumačiti s obzirom na sudsku praksu Suda tako da se u potpunosti odražavaju ciljevi ove Uredbe”⁶⁵¹. Voditelji obrade snose odgovornost i mogu biti izloženi zahtjevima za naknadu štete ako ne ispunjavaju svoje obveze na temelju Uredbe. Izvršitelji obrade osobnih podataka odgovorni su za štetu uzrokovanu obradom samo kada ona nije bila u skladu s obvezama iz Uredbe koje se izričito odnose na izvršitelje obrade ili kada je provedena mimo zakonitih uputa voditelja obrade ili protivno njima. Ako je voditelj obrade ili izvršitelj obrade

⁶⁴⁹ Opća uredba o zaštiti podataka, članak 80.

⁶⁵⁰ *Ibid.*, članak 82.

⁶⁵¹ *Ibid.*, uvodna izjava 146.

platio punu odštetu, OUZP-om se utvrđuje da taj voditelj obrade ili izvršitelj obrade može zatražiti od drugih voditelja obrade ili izvršitelja obrade koji su uključeni u istu obradu da plate dio odštete koji odgovara njihovu udjelu u odgovornosti za štetu⁶⁵². Izuzeća od odgovornosti vrlo su stroga i zahtijevaju dokaz da voditelj ili izvršitelj obrade ni na koji način nije odgovoran za događaj koji je prouzročio štetu.

Naknada mora biti „potpuna i učinkovita” s obzirom na pretrpljenu štetu. Ako je šteta uzrokovana obradom nekoliko voditelja obrade ili izvršitelja obrade, svaki voditelj obrade ili izvršitelj obrade mora snositi odgovornost za svu štetu. Tim se pravilom nastoji osigurati učinkovita naknada za ispitanike i koordinirani pristup sukladnosti voditelja obrade i izvršitelja obrade koji sudjeluju u aktivnostima obrade.

Primjer: Ispitanici ne moraju pokrenuti postupak i zatražiti naknadu štete od svih tijela odgovornih za štetu jer to može podrazumijevati visoke troškove i dugotrajne postupke. Dovoljno je pokrenuti postupak protiv jednog od zajedničkih voditelja obrade, koji će snositi odgovornost za svu štetu. U takvim slučajevima voditelj obrade ili izvršitelj obrade koji plati odštetu naknadno ima pravo na povrat dijela plaćenog iznosa od drugih tijela uključenih u obradu i odgovornih za kršenje proporcionalno njihovu dijelu odgovornosti za štetu. Ti postupci između različitih zajedničkih voditelja obrade i izvršitelja obrade odvijaju se nakon što ispitanik primi naknadu te on u njima ne sudjeluje.

Unutar pravnog okvira Vijeća Europe, člankom 12. modernizirane Konvencije br. 108 propisuje se da ugovorne stranke uspostave odgovarajuće pravne lijekove za kršenje nacionalnog prava kojim se provode odredbe Konvencije. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da pravni lijekovi moraju uključivati mogućnost sudskog preispitivanja odluke ili prakse te da moraju biti dostupni i izvansudski pravni lijekovi⁶⁵³. Odluke o pojedinim modalitetima i pravilima povezanim s pristupom tim pravnim lijekovima, kao i postupci koje treba slijediti, prepušteni su svakoj ugovornoj stranci. Ugovorne stranke i nacionalni sudovi trebaju razmotriti i uvođenje odredbi o novčanoj naknadi za materijalnu i nematerijalnu štetu uzrokovanu obradom, kao i mogućnost pokretanja kolektivnih postupaka⁶⁵⁴.

652 *Ibid.*, članak 82. stavci 2. i 5.

653 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 100.

654 *Ibid.*

6.2.4. Sankcije

Unutar prava Vijeća Europe, člankom 12. modernizirane Konvencije br. 108 propisano je da svaka ugovorna stranka mora uspostaviti odgovarajuće sankcije i pravne lijekove za kršenja odredbi domaćeg zakonodavstva kojima se provode osnovna načela zaštite podataka utvrđena u Konvenciji br. 108. Konvencijom se ne uspostavlja niti nameću određene sankcije. Upravo suprotno, u njoj se jasno ističe da svaka ugovorna stranka prema vlastitom nahođenju može odrediti prirodu sudskih i izvan-sudskih sankcija, koje mogu biti kaznene, upravne ili građanskopravne. U Izvješću s objašnjenjima o moderniziranoj Konvenciji br. 108 navodi se da sankcije moraju biti učinkovite, proporcionalne i odvraćajuće⁶⁵⁵. Ugovorne stranke moraju se pridržavati tog načela pri određivanju prirode i težine sankcija koje su dostupne na temelju njihova nacionalnog pravnog poretka.

Unutar prava EU-a, člankom 83. OUZP-a nadzorna tijela država članica ovlašćuju se za izricanje upravnih novčanih kazni za kršenja Uredbe. Iznos novčanih kazni, okolnosti koje nacionalna tijela moraju uzeti u obzir pri odlučivanju o izricanju kazne te ukupne gornje granice iznosa novčanih kazni također su propisani člankom 83. Sustav izricanja sankcija tako je usklađen u cijelom EU-u.

U OUZP-u se primjenjuje pristup novčanim kaznama temeljen na više razina. Nadzorna tijela imaju ovlast izricanja upravnih novčanih kazni za kršenja Uredbe u iznosu do 20 000 000 € ili, u slučaju poduzeća, 4 % od ukupnog godišnjeg prometa na svjetskoj razini, ovisno o tome što je veće. Kršenja za koja se može izreći ta razina novčane kazne uključuju povrede osnovnih načela za obradu i uvjeta privole, povrede prava ispitanika i odredbi Uredbe kojima se uređuje prijenos osobnih podataka primateljima u trećim zemljama. Za druga kršenja nadzorna tijela mogu izreći novčane kazne u iznosu do 10 000 000 € ili, u slučaju poduzeća, 2 % od ukupnog godišnjeg prometa na svjetskoj razini, ovisno o tome što je veće.

Pri određivanju vrste i razine novčane kazne koja se izriče, nadzorna tijela moraju uzeti u obzir niz čimbenika⁶⁵⁶. Primjerice, moraju posvetiti pozornost naravi, ozbiljnosti i trajanju kršenja, kategorijama zahvaćenih osobnih podataka te ima li kršenje obilježje namjere ili nepažnje. U obzir također treba uzeti svaku radnju koju je voditelj ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici. Drugi su važni čimbenici koji nadzornim tijelima pomažu u donošenju odluke stupanj suradnje

⁶⁵⁵ *Ibid.*

⁶⁵⁶ Opća uredba o zaštiti podataka, članak 83. stavak 2.

s nadzornim tijelom nakon kršenja, način na koji je nadzorno tijelo doznalo za kršenje (primjerice, je li o njemu izvijestilo tijelo nadležno za obradu ili ispitanik)⁶⁵⁷.

Uz mogućnost izricanja upravnih novčanih kazni, nadzorna tijela na raspolaganju imaju širok niz drugih korektivnih mjera. Takozvane „korektivne” ovlasti nadzornih tijela utvrđene su člankom 58. OUZP-a. One uključuju izdavanje naredbi, upozorenja i službenih opomena voditeljima obrade i izvršiteljima obrade te privremenu ili čak trajnu zabranu aktivnosti obrade.

U pogledu sankcija protiv kršenja prava Unije koja počine institucije ili tijela EU-a, zbog posebne ovlasti Uredbe o zaštiti podataka u institucijama Europske unije, sankcije mogu biti predviđene samo u obliku disciplinskih mjera. Prema članku 49. te Uredbe, „[s]vaki propust u poštovanju obveza prema ovoj Uredbi, bilo da je namjeran ili posljedica nemara dužnosnika ili nekog drugog službenika Europskih zajednica, čini ih podložnima stegovnom postupku [...]”.

⁶⁵⁷ Radna skupina iz članka 29. (2017.), *Smjernice o primjeni i određivanju upravnih novčanih kazni za potrebe Uredbe 2016/679*, WP 253, 3. listopada 2017.

7

Međunarodni prijenos podataka i protok osobnih podataka

EU	Obuhvaćena pitanja	Vijeće Europe
Prijenosi osobnih podataka		
Opća uredba o zaštiti podataka, članak 44.	Koncept	Modernizirana Konvencija br. 108, članak 14. stavci 1. i 2.
Slobodan protok osobnih podataka		
Opća uredba o zaštiti podataka, članak 1. stavak 3. i uvodna izjava 170.	Među državama članicama Europske unije	
	Među ugovornim strankama Konvencije br. 108	Modernizirana Konvencija br. 108, članak 14. stavak 1.
Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama		
Opća uredba o zaštiti podataka, članak 45. C-362/14, <i>Maximillian Schrems protiv Data Protection Commissioner</i> [VV], 2015.	Odluka o primjerenosti / treće zemlje ili međunarodne organizacije s odgovarajućim razinama zaštite	Modernizirana Konvencija br. 108, članak 14. stavak 2.
Opća uredba o zaštiti podataka, članak 46. stavak 1. i članak 46. stavak 2.	Odgovarajuće zaštitne mjere, uključujući provediva prava i pravne lijekove za ispitanike, koje se pružaju putem standardnih ugovornih klauzula, obvezujućih korporativnih pravila, kodeksa ponašanja i mehanizama certificiranja	Modernizirana Konvencija br. 108, članak 14. stavci 2., 3., 5. i 6.

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka, članak 46. stavak 3.	Uvjetovano odobrenjem nadležnog nadzornog tijela: ugovorne klauzule i odredbe sadržane u administrativnim dogovorima između javnih tijela	
Opća uredba o zaštiti podataka, članak 46. stavak 5.	Postojeća odobrenja na temelju Direktive 95/46/EZ	
Opća uredba o zaštiti podataka, članak 47.	Obvezujuća korporativna pravila	
Opća uredba o zaštiti podataka, članak 49.	Odstupanja za posebne situacije	Modernizirana Konvencija br. 108, članak 14. stavak 4.
Primjeri: Sporazum između EU-a i SAD-a o podacima iz evidencije podataka o putnicima Sporazum SWIFT između EU-a i SAD-a	Međunarodni sporazumi	Modernizirana Konvencija br. 108, članak 14. stavak 3. točka (a)

U okviru prava Unije, Općom uredbom o zaštiti podataka uređuje se slobodan protok podataka unutar Europske unije. Međutim, ona sadržava posebne zahtjeve koji se odnose na prijenose osobnih podataka trećim zemljama izvan EU-a i međunarodnim organizacijama. Uredbom se potvrđuje važnost takvih prijenosa, posebno u kontekstu međunarodne trgovine i suradnje, no prepoznaje se i povećan rizik za osobne podatke. Uredbom se stoga nastoji pružiti razina zaštite za prijenos osobnih podataka u treće zemlje koja je jednaka onoj unutar EU-a⁶⁵⁸. Pravom Vijeća Europe također se potvrđuje važnost provedbe pravila za prekogranične prijenose podataka na temelju slobodnog protoka među strankama i posebnih zahtjeva za prijenose drugim stranama.

658 Opća uredba o zaštiti podataka, uvodne izjave 101. i 116.

7.1. Priroda prijenosa osobnih podataka

Ključne točke

- Europska unija i Vijeće Europe imaju propise o prijenosima osobnih podataka primateljima u trećim zemljama ili međunarodnim organizacijama.
- Osiguravanjem zaštite prava ispitanika prilikom prijenosa podataka izvan EU-a omogućuje se zadržavanje zaštite propisane pravom EU-a za osobne podatke podrijetlom iz EU-a.

Prema **pravu Vijeća Europe**, prekogranični prijenosi podataka opisuju se kao prijenosi osobnih podataka primateljima koji podliježu nadležnosti drugih država⁶⁵⁹. Prekogranični prijenosi podataka primatelju koji ne podliježe nadležnosti ugovorne stranke dozvoljeni su samo ako je prisutna odgovarajuća razina zaštite⁶⁶⁰.

Pravom EU-a uređuju se prijenosi „osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju [...]”⁶⁶¹. Takvi su prijenosi podataka dopušteni samo ako su usklađeni s pravilima iz poglavlja V. OUZP-a.

Prekogranični prijenosi osobnih podataka dopušteni su prema primateljima koji podliježu nadležnosti ugovorne stranke Vijeća Europe ili države članice EU-a. U obama pravnim sustavima dopušta se prijenos podataka u zemlju koja nije ugovorna stranka ni država članica ako su ispunjeni određeni uvjeti.

659 Izvješće s objašnjenjima o moderniziranoj Konvenciji br. 108, stavak 102.

660 Modernizirana Konvencija br. 108, članak 14. stavak 2.

661 Opća uredba o zaštiti podataka, članak 44.

7.2. Slobodno kretanje/protok osobnih podataka među državama članicama ili ugovornim strankama

Ključne točke

- Protok osobnih podataka kroz EU i prijenosi osobnih podataka među ugovornim strankama modernizirane Konvencije br. 108 ne smiju biti ograničeni. Međutim, budući da nisu sve ugovorne stranke modernizirane Konvencije br. 108 države članice EU-a, prijenosi iz države članice EU-a u treću zemlju koja jest ugovorna stranka modernizirane Konvencije br. 108 nisu mogući ako ne ispunjavaju uvjete utvrđene OUZP-om.

Prema pravu Vijeća Europe, mora se osigurati slobodan protok osobnih podataka među ugovornim strankama modernizirane Konvencije br. 108. Međutim, prijenos može biti zabranjen ako postoji „stvaran i ozbiljan rizik da bi prijenos drugoj stranci doveo do zaobilaženja odredbi Konvencije” ili ako je stranka obvezna to učiniti sukladno „usklađenim pravilima zaštite među državama koje pripadaju regionalnoj međunarodnoj organizaciji”⁶⁶².

Unutar prava EU-a slobodno kretanje osobnih podataka među državama članicama EU-a ne ograničava se niti zabranjuje iz razloga povezanih sa zaštitom pojedinaca u pogledu obrade osobnih podataka⁶⁶³. **Područje slobodnog prijenosa podataka prošireno je** Sporazumom o europskom gospodarskom prostoru (EGP)⁶⁶⁴, kojim se Island, Lihtenštajn i Norveška uvode na unutarnje tržište.

Primjer: Ako podružnica međunarodne grupacije s poslovnim nastanom u nekoliko država članica, među ostalim u Sloveniji i Francuskoj, pošalje osobne podatke iz Slovenije u Francusku, takav se prijenos podataka ne smije ograničiti ni zabraniti slovenskim nacionalnim zakonodavstvom iz razloga povezanih sa zaštitom osobnih podataka.

⁶⁶² Modernizirana Konvencija br. 108, članak 14. stavak 1.

⁶⁶³ Opća uredba o zaštiti podataka, članak 1. stavak 3.

⁶⁶⁴ Odluka Vijeća i Komisije od 13. prosinca 1993. o sklapanju Sporazuma o Europskom gospodarskom prostoru između Europskih zajednica, njihovih država članica i Republike Austrije, Republike Finske, Republike Islanda, Kneževine Lihtenštajna, Kraljevine Norveške, Kraljevine Švedske i Švicarske Konfederacije, SL 1994 L 1.

Međutim, ako ista slovenska podružnica želi prenijeti te osobne podatke matičnom društvu u Maleziji, slovenski izvoznik podataka mora uzeti u obzir pravila iz poglavlja V. OUZP-a. Tim se odredbama nastoje zaštititi osobni podaci ispitanika koji podliježu nadležnosti EU-a.

Prema pravu Unije, prijenosi osobnih podataka u države članice EGP-a u svrhe povezane sa sprečavanjem, istragom, otkrivanjem ili progonom kaznenih djela ili izvršavanjem kaznenih sankcija podliježu Direktivi (EU) 2016/680⁶⁶⁵. Time se također osigurava da razmjena osobnih podataka među nadležnim tijelima unutar Unije nije ograničena ni zabranjena iz razloga zaštite podataka. Prema pravu Vijeća Europe, obrada svih osobnih podataka (uključujući prekogranični prijenos drugim strankama Konvencije br. 108), bez iznimki na temelju svrha ili područja djelovanja, obuhvaćena je područjem primjene Konvencije br. 108, iako ugovorne stranke mogu uvesti izuzeća. Svi članovi EGP-a također su stranke Konvencije br. 108.

7.3. Prijenosi osobnih podataka trećim zemljama/zemljama koje nisu stranke ili međunarodnim organizacijama

Ključne točke

- **I Vijeće Europe i EU** dopuštaju prijenose osobnih podataka trećim zemljama ili međunarodnim organizacijama ako su ispunjeni određeni uvjeti za zaštitu osobnih podataka.
- **Prema pravu Vijeća Europe**, odgovarajuća razina zaštite može se postići zakonodavstvom države ili međunarodne organizacije ili uspostavljanjem odgovarajućih standarda.
- **Prema pravu EU-a**, prijenosi se mogu odvijati ako treća zemlja osigura odgovarajuću razinu zaštite ili ako voditelj obrade podataka ili izvršitelj obrade pruži odgovarajuće zaštitne mjere, uključujući provediva prava i pravne lijekove za ispitanika, u obliku standardnih ugovornih klauzula ili obvezujućih korporativnih pravila.
- **I jednim i drugim pravom** predviđene su klauzule o odstupanju kojima se omogućuje prijenos osobnih podataka u posebnim okolnostima, čak i kada ne postoje odgovarajuća razina zaštite ni odgovarajuće zaštitne mjere.

⁶⁶⁵ Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL 2016 L119.

Iako se i pravom Vijeća Europe i pravom EU-a dopuštaju prijenosi podataka trećim zemljama ili međunarodnim organizacijama, utvrđuju se različiti uvjeti. U svakom se skupu uvjeta u obzir uzimaju različite strukture i svrhe pojedinih organizacija.

U sklopu **prava EU-a** u načelu postoje dva načina na koja je moguć prijenos osobnih podataka u treće zemlje ili međunarodne organizacije. Prijenosi osobnih podataka mogu se obavljati na temelju odluke o primjerenosti Europske komisije⁶⁶⁶ ili, u nedostatku takve odluke, kada voditelj obrade ili izvršitelj obrade pruži odgovarajuće zaštitne mjere, uključujući provediva prava i pravne lijekove za ispitanika⁶⁶⁷. U nedostatku odluke o primjerenosti ili odgovarajućih zaštitnih mjera, moguća su brojna odstupanja.

Međutim, sukladno pravu **Vijeća Europe**, slobodni prijenosi podataka državama koje nisu stranke Konvencije dopušteni su samo na temelju:

- zakona te države ili međunarodne organizacije, uključujući primjenjive međunarodne ugovore ili sporazume kojima se jamče odgovarajuće zaštitne mjere,
- *ad hoc* ili odobrenih standardiziranih zaštitnih mjera utvrđenih pravno obvezujućim i provedivim instrumentima koje donose i provode osobe uključene u prijenos i daljnju obradu⁶⁶⁸.

Slično kao i unutar prava EU-a, u nedostatku odgovarajuće razine zaštite podataka, dostupna su brojna odstupanja.

7.3.1. Prijenosi na temelju odluke o primjerenosti

Unutar prava EU-a slobodan prijenos podataka trećim zemljama s odgovarajućom razinom zaštite podataka predviđen je člankom 45. OUZP-a. SEU je pojasnio da pojam „odgovarajuća razina zaštite” podrazumijeva da treća zemlja osigurava razinu zaštite temeljnih prava i sloboda koja je „u načelu istovjetna”⁶⁶⁹ jamstvima osiguranim pravom Unije. Istovremeno, sredstva kojima se koristi treća zemlja za

⁶⁶⁶ Opća uredba o zaštiti podataka, članak 45.

⁶⁶⁷ *Ibid.*, članak 46.

⁶⁶⁸ Modernizirana Konvencija br. 108, članak 14. stavak 3. točke (a) i (b).

⁶⁶⁹ SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [W], 6. listopada 2015., t. 96.

osiguravanje takve razine zaštite mogu se razlikovati od onih koja se provode u EU-u jer se standardom primjerenosti ne zahtijeva potpuno preslikavanje propisa EU-a⁶⁷⁰.

Europska komisija procjenjuje razinu zaštite podataka u drugim zemljama razmatranjem njihova nacionalnog zakonodavstva i primjenjivih međunarodnih obveza. U obzir uzima i sudjelovanje pojedine države u multilateralnim ili regionalnim sustavima, posebice u vezi sa zaštitom osobnih podataka. Ako Europska komisija zaključi da treća zemlja ili međunarodna organizacija osigurava odgovarajuću razinu zaštite, može izdati odluku o primjerenosti koja ima obvezujući učinak⁶⁷¹. Međutim, SEU je ustvrdio da su nacionalna nadzorna tijela ipak nadležna za ispitivanje zahtjeva određene osobe u vezi sa zaštitom njezinih osobnih podataka koji su preneseni u treću zemlju za koju je Komisija utvrdila da osigurava odgovarajuću razinu zaštite, nastavno na navode te osobe da važeće pravo i praksa u toj trećoj zemlji ne osiguravaju odgovarajuću razinu zaštite⁶⁷².

Europska komisija također može procijeniti primjerenost državnog područja u trećoj zemlji ili se ograničiti na pojedine sektore, kao što je bio slučaj s kanadskim zakonodavstvom o privatnoj komercijalnoj djelatnosti⁶⁷³. Odluke o primjerenosti za prijenose mogu se donositi i na temelju sporazuma između EU-a i trećih zemalja. Te se odluke odnose isključivo na jednu vrstu prijenosa podataka, kao što su evidencije podataka o putnicima koje zračne kompanije prenose stranim tijelima za graničnu kontrolu kada zrakoplov leti iz Europske unije u određena prekomorska odredišta (vidjeti dio 7.3.4.).

Odluke o primjerenosti podliježu stalnom nadzoru. Europska komisija redovito preispituje takve odluke kako bi pratila razvoj događaja koji bi mogli utjecati na njihov status. Stoga ako Europska komisija utvrdi da treća zemlja ili međunarodna organizacija više ne ispunjava uvjete iz odluke o primjerenosti, odluku može izmijeniti, obustaviti ili staviti izvan snage. Komisija također može pokrenuti pregovore s predmetnom trećom zemljom ili međunarodnom organizacijom kako bi riješila problem iz odluke.

670 *Ibid.*, t. 74. Vidjeti i Europska komisija (2017.), Komunikacija Komisije Europskom parlamentu i Vijeću „Razmjena i zaštita osobnih podataka u globaliziranom svijetu“, COM(2017) 7 final od 10. siječnja 2017., str. 6.

671 Popis zemalja za koje je donesena odluka o primjerenosti, koji se redovito ažurira, potražite na početnoj stranici [Glavne uprave za pravosuđe Europske komisije](#).

672 SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VW], 6. listopada 2015., t. 63., 65. i 66.

673 Europska Komisija (2002.), Odluka 2002/2/EZ od 20. prosinca 2001. u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o odgovarajućoj zaštiti osobnih podataka propisanoj u Zakonu o zaštiti osobnih podataka i elektroničkih dokumenata Kanade, SL 2002 L 2.

Odluke o primjerenosti koje Europska komisija donese na temelju Direktive 95/46/EZ ostaju na snazi dok se ne izmijene, zamijene ili stave izvan snage odlukom Komisije donesenom u skladu s pravilima iz članka 45. OUZP-a.

Do sada je Europska komisija donijela odluku da primjerenu zaštitu pružaju Andora, Argentina, Kanada (komercijalne organizacije koje su obuhvaćene područjem primjene kanadskog Zakona o zaštiti osobnih podataka i o elektroničkim dokumentima, odnosno *Personal Information and Electronic Documents Act* – PIPEDA), Farski otoci, Guernsey, Otok Man, Izrael, Jersey, Novi Zeland, Švicarska i Urugvaj. U pogledu prijenosa podataka u SAD, Europska komisija donijela je odluku o primjerenosti 2000., kojom su omogućeni prijenosi društvima koja sama potvrđuju da će štititi osobne podatke prenesene iz EU-a i pridržavati se tzv. „načela sigurne luke”⁶⁷⁴. SEU je poništio tu odluku 2015. te je u srpnju 2016. donesena nova odluka o primjerenosti kojom je društvima dopušteno da se pridruže od 1. kolovoza 2016.

Primjer: U predmetu *Schrems*⁶⁷⁵ austrijski državljani Maximillian Schrems bio je višegodišnji korisnik društvene mreže Facebook. Neki ili svi podaci koje je g. Schrems pružio Facebooku preneseni su iz irske podružnice Facebooka na poslužitelje u SAD-u, gdje su i obrađeni. G. Schrems podnio je pritužbu irskom nadležnom tijelu za zaštitu podataka, smatrajući da, s obzirom na otkrića američkog zviždača Edwarda Snowdena o aktivnostima nadzora obavještajnih službi SAD-a, zakoni i praksa SAD-a ne pružaju dostatnu zaštitu za podatke prenesene u tu zemlju. Irsko je tijelo odbacilo pritužbu pozivajući se činjenicu da je Komisija u svojoj Odluci od 26. srpnja 2000. utvrdila da SAD osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka u sklopu sustava „sigurne luke”. Predmet je iznesen pred irskim Visokim sudom, koji ga je uputio SEU-u radi prethodne odluke.

SEU je presudio da je Komisijina odluka o primjerenosti okvira „sigurne luke” nevaljana. Prvo je istaknuo da je odlukom dopušteno ograničenje primjenjivosti načela „sigurne luke” za zaštitu podataka na temelju nacionalne sigurnosti, javnog interesa ili uvjeta za provedbu zakona ili na temelju nacionalnog zakonodavstva u SAD-u. Odlukom je stoga omogućeno miješanje u temeljna

674 Odluka Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a, SL L 215. SEU je Odluku proglasio nevaljanom u predmetu C-632/14, *Maximillian Schrems protiv Data Protection Commissioner* [VW].

675 SEU, C-362/14, *Maximillian Schrems protiv Data Protection Commissioner* [VW], 6. listopada 2015.

prava osoba čiji su osobni podaci preneseni ili bi mogli biti preneseni u SAD⁶⁷⁶. Zatim je napomenuo da odluka ne sadržava nikakvo utvrđenje o postojanju pravila SAD-a za ograničavanje takva miješanja u temeljna prava ni o bilo kakvoj učinkovitoj pravnoj zaštiti protiv miješanja takve naravi⁶⁷⁷. SEU je naglasio da razina zaštite temeljnih prava i sloboda zajamčenih u Europskoj uniji zahtijeva da se u propisima kojima se zadire u temeljna prava zajamčena u člancima 7. i 8. predvide jasna i precizna pravila koja uređuju doseg i primjenu mjere te propišu minimalne zaštitne mjere, odstupanja i ograničenja u zaštiti osobnih podataka⁶⁷⁸. Budući da u Odluci Komisije nije utvrđeno da SAD doista osigurava odgovarajuću razinu zaštite na temelju svojeg domaćeg zakonodavstva ili međunarodnih obveza koje je preuzeo, SEU je zaključio da ne ispunjava zahtjeve relevantne odredbe o prijenosu iz Direktive o zaštiti podataka te da stoga nije valjana⁶⁷⁹.

Razina zaštite u SAD-u stoga nije bila „u načelu istovjetna” temeljnim pravima i slobodama osiguranim pravom Unije⁶⁸⁰. SEU je utvrdio da je prekršeno više članaka Povelje EU-a o temeljnim pravima. Za početak, povrijeđen je bitan sadržaj članka 7. s obzirom na to da propis SAD-a „omogućava javnim tijelima općenit pristup sadržaju elektroničkih komunikacija”. Zatim je prekršen i bitan sadržaj članka 47. jer propisom pojedincima nije pružena nikakva mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima ili radi ispravka ili brisanja osobnih podataka. Naposljetku, budući da su sustavom „sigurne luke” prekršeni navedeni članci, osobni podaci nisu zakonito obrađeni, što je dovelo do kršenja članka 8.

Nakon što je SEU proglasio sustav „sigurne luke” nevaljanim, Komisija i SAD postigli su sporazum o novom okviru, europsko-američkom sustavu zaštite privatnosti (engl. *EU-US Privacy Shield*). Komisija je 12. srpnja 2016. donijela odluku kojom je obznanila

676 *Ibid.*, t. 84.

677 *Ibid.*, t. 88. i 89.

678 *Ibid.*, t. 91. i 92.

679 *Ibid.*, t. 96. i 97.

680 *Ibid.*, t. 73., 74. i 96.

da SAD osigurava odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije u organizacije u SAD-u u sklopu sustava zaštite privatnosti⁶⁸¹.

Slično kao i sporazumom o „sigurnoj luci“, okvirom europsko-američkog sustava za zaštitu privatnosti nastoje se zaštititi osobni podaci koji se prenose iz EU-a u SAD u komercijalne svrhe⁶⁸². Društva u SAD-u mogu obaviti dobrovoljno samocertificiranje pridržavanja popisa iz sustava za zaštitu privatnosti tako da se obvežu na ispunjavanje standarda zaštite podataka tog okvira. Nadležna tijela u SAD-u nadziru i provjeravaju sukladnost certificiranih društava s tim standardima.

Sustavom za zaštitu privatnosti posebno se utvrđuje sljedeće:

- obveze zaštite podataka za poduzeća koja primaju osobne podatke iz EU-a,
- zaštita i mogućnosti za ostvarivanje pravne zaštite pojedinaca, posebice uspostava mehanizma pravobranitelja, koji djeluje neovisno od obavještajnih službi SAD-a i obrađuje pritužbe pojedinaca koji smatraju da su tijela SAD-a nadležna za nacionalnu sigurnost nezakonito upotrijebila njihove osobne podatke,
- godišnje zajedničko preispitivanje kojim se nadzire provedba okvira⁶⁸³; prvo je preispitivanje održano u rujnu 2017.⁶⁸⁴

Vlada SAD-a dopunila je odluku o sustavu za zaštitu privatnosti pisanim obvezama i jamstvima. Njima se utvrđuju ograničenja i zaštitne mjere za pristup vlade SAD-a osobnim podacima u svrhu izvršavanja zakonodavstva i nacionalne sigurnosti.

681 [Provedbena odluka Komisije \(EU\) 2016/1250](#) od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL L 207. Radna skupina iz članka 29. pozdravila je poboljšanja koja su uvedena tim mehanizmom zaštite privatnosti u odnosu na odluku o „sigurnoj luci“ te je pohvalila Komisiju i nadležna tijela SAD-a jer su u završnoj verziji dokumenata o sustavu zaštite privatnosti uzeli u obzir pitanja iznesena u njezinu mišljenju WP 238 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti. Unatoč tome, Radna skupina istaknula je niz neriješenih pitanja. Više pojedinosti dostupno je u: Radna skupina iz članka 29., Mišljenje 01/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava za zaštitu privatnosti, doneseno 13. travnja 2016., 16/EN WP 238.

682 Više informacije dostupno je u dokumentu [EU-U.S. Privacy Shield factsheet](#) (Informativni list o europsko-američkom sustavu za zaštitu privatnosti).

683 Više informacija dostupno je na internetskoj stranici Europske komisije [EU-U.S. Privacy Shield factsheet](#).

684 Europska komisija, [Izješće Komisije Europskom Parlamentu i Vijeću o prvom godišnjem preispitivanju funkcioniranja europsko-američkog sustava zaštite privatnosti](#), COM(2017) 611 final, 18. listopada 2017. Vidjeti i Radna skupina iz članka 29., [Prvo godišnje preispitivanje funkcioniranja europsko-američkog sustava zaštite privatnosti](#), doneseno 28. studenoga 2017., 17/EN WP 255.

7.3.2. Prijenosi koji podliježu odgovarajućim zaštitnim mjerama

I u **pravu EU-a** i u **pravu Vijeća Europe** utvrđuju se odgovarajuće zaštitne mjere između voditelja obrade koji izvozi podatke i primatelja u trećoj zemlji ili međunarodne organizacije. Takve mjere navode se kao mogući način osiguravanja odgovarajuće razine zaštite podataka za primatelja.

Sukladno **pravu EU-a**, prijenosi osobnih podataka u treću zemlju ili međunarodnu organizaciju dopušteni su ako voditelj ili izvršitelj obrade osigurava odgovarajuće zaštitne mjere i provediva prava te ako su ispitanicima dostupni učinkoviti pravni lijekovi⁶⁸⁵. Popis „odgovarajućih zaštitnih mjera” propisan je isključivo zakonodavstvom EU-a o zaštiti podataka. Odgovarajuće zaštitne mjere mogu se uspostaviti na sljedeće načine:

- pravno obvezujućim i provedivim instrumentima između tijela javne vlasti ili javnih tijela,
- obvezujućim korporativnim pravilima,
- standardnim klauzulama o zaštiti podataka koje donosi Europska komisija ili nadzorno tijelo,
- kodeksima ponašanja,
- mehanizmima certificiranja⁶⁸⁶.

Posebne ugovorne klauzule između voditelja obrade ili izvršitelja obrade u EU-u i primatelja podataka u trećoj zemlji dodatan su način osiguravanja odgovarajućih zaštitnih mjera. Međutim, takve ugovorne klauzule mora odobriti nadležno nadzorno tijelo prije nego što se budu mogle primijeniti kao sredstvo prijenosa osobnih podataka. Jednako tako, javna tijela mogu iskoristiti odredbe o zaštiti podataka uvrštene u njihove administrativne dogovore ako ih nadzorno tijelo odobri⁶⁸⁷.

685 Opća uredba o zaštiti podataka, članak 46.

686 *Ibid.*, članak 46. stavak 1. točke (c) i (d), članak 46. stavak 2. točke (a), (b), (e) i (f) te članak 47.

687 *Ibid.*, članak 46. stavak 3.

Sukladno pravu Vijeća Europe, prijenosi podataka u državu ili međunarodnu organizaciju koja nije ugovorna stranka modernizirane Konvencije br. 108 dopušteni su pod uvjetom da se osigura odgovarajuća razina zaštite. To se može postići:

- zakonom države ili međunarodne organizacije, ili
- *ad hoc* ili standardiziranim zaštitnim mjerama ugrađenima u pravno obvezujući dokument⁶⁸⁸.

Prijenosi koji podliježu ugovornim klauzulama

I u **pravu Vijeća Europe** i u **pravu EU-a** utvrđuju se ugovorne klauzule kojima se vezuju voditelj obrade koji izvozi podatke i primatelj u trećoj zemlji. Takve klauzule navode se kao mogući način osiguravanja odgovarajuće razine zaštite podataka za primatelja⁶⁸⁹.

Na **razini EU-a** Europska komisija uz pomoć Radne skupine iz članka 29. razvila je standardne klauzule o zaštiti podataka koje su službeno ovjerene odlukom Komisije kao dokaz odgovarajuće razine zaštite podataka⁶⁹⁰. Budući da su odluke Komisije u cijelosti obvezujuće u državama članicama, nacionalna tijela nadležna za nadzor prijenosa podataka moraju potvrditi te standardne ugovorne klauzule u svojim postupcima⁶⁹¹. Stoga ako se voditelj obrade koji izvozi podatke i primatelj iz treće zemlje dogovore i potpišu te klauzule, to bi za nadzorno tijelo trebao biti dovoljan dokaz provođenja odgovarajućih zaštitnih mjera. Međutim, u predmetu *Schrems* SEU je smatrao da Europska komisija nije nadležna za ograničenje ovlasti nacionalnih nadzornih tijela da nadziru prijenos osobnih podataka u treću zemlju koja je bila predmet odluke Komisije o primjerenosti⁶⁹². Stoga se nacionalna nadzorna tijela ne sprečava da izvršavaju svoje ovlasti, uključujući ovlast da suspendiraju ili zabrane prijenos osobnih podataka kada se prijenosom krši zakonodavstvo EU-a ili

688 Modernizirana Konvencija br. 108, članak 14. stavak 3. točka (b).

689 Opća uredba o zaštiti podataka, članak 46. stavak 3.; modernizirana Konvencija br. 108, članak 14. stavak 3. točka (b).

690 Opća uredba o zaštiti podataka, članak 46. stavak 2. točka (b) i članak 46. stavak 5.

691 *Ibid.*, članak 46. stavak 2. točka (c); Ugovor o funkcioniranju Europske unije, članak 288.

692 SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VV], 6. listopada 2015., t. od 96. do 98. i od 102. do 105.

nacionalno zakonodavstvo o zaštiti podataka, primjerice kada se uvoznik podataka ne pridržava standardnih ugovornih klauzula⁶⁹³.

Postojanje standardnih klauzula o zaštiti podataka u pravnom okviru EU-a ne sprečava voditelje obrade da utvrde druge *ad hoc*, pojedinačne ugovorne klauzule, pod uvjetom da ih odobri nadležno nadzorno tijelo⁶⁹⁴. Međutim, tim bi klauzulama trebali osigurati jednaku razinu zaštite koju osiguravaju standardne klauzule o zaštiti podataka. Prilikom odobravanja *ad hoc* klauzula, nadzorna tijela moraju primijeniti mehanizam konzistentnosti kako bi se osigurao dosljedan regulatorni pristup na razini EU-a⁶⁹⁵. To znači da nadležno nadzorno tijelo mora EOZP obavijestiti o svojem nacrtu odluke o klauzulama. EOZP će o tome dati mišljenje, a nadzorno tijelo mora u najvećoj mogućoj mjeri uzeti u obzir to mišljenje prilikom donošenja odluke. Ako tijelo ne namjerava slijediti mišljenje EOZP-a, aktivirat će se mehanizam rješavanja sporova unutar EOZP-a i Odbor će donijeti obvezujuću odluku⁶⁹⁶.

Najvažnije značajke standardnih ugovornih klauzula jesu:

- klauzula o korisniku trećoj strani kojom se ispitanicima omogućuje ostvarivanje ugovornih prava iako nisu stranke ugovora,
- primatelj ili uvoznik podataka pristaje na podvrgavanje ovlastima nacionalnog nadzornog tijela i/ili sudova voditelja obrade koji izvozi podatke u slučaju spora.

Dostupna su dva skupa standardnih klauzula za prijenose između dvaju voditelja obrade koje voditelj obrade može odabrati⁶⁹⁷. Za prijenose između voditelja i izvrši-

693 Kako bi uzela u obzir stajalište SEU-a u predmetu *Schrems*, Komisija je izmijenila svoju Odluku o standardnim ugovornim klauzulama. [Provedbena odluka Komisije \(EU\) 2016/2297](#) od 16. prosinca 2016. o izmjeni odluka 2001/497/EZ i 2010/87/EU o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje i obrađivačima u tim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL 2016 L344.

694 Opća uredba o zaštiti podataka, članak 46. stavak 3. točka (a).

695 *Ibid.*, članak 63. i članak 64. stavak 1. točka (e).

696 *Ibid.*, članak 64. i članak 65.

697 Skup I. nalazi se u Prilogu Odluci Komisije 2001/497/EZ od 15. lipnja 2001. (Europska komisija (2001)) o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje, u skladu s Direktivom 95/46/EZ, SL 2001 L 181; skup II. nalazi se u Prilogu Odluci Komisije 2004/915/EZ od 27. prosinca 2004. (Europska komisija (2004)) o izmjeni Odluke 2001/497/EZ u pogledu uvođenja alternativnog skupa standardnih ugovornih klauzula za prijenos osobnih podataka u treće zemlje, SL 2004 L 385.

telja obrade postoji samo jedan skup standardnih ugovornih klauzula⁶⁹⁸. Međutim, te su standardne ugovorne klauzule trenutačno predmet sudskog postupka.

Primjer: Nakon što je SEU proglasio odluku o „sigurnoj luci” nevaljanom⁶⁹⁹, prijenosi osobnih podataka u SAD više se ne mogu temeljiti na toj odluci o primjerenosti. Tijekom pregovora s tijelima SAD-a i u očekivanju donošenje nove odluke o primjerenosti (koja je naposljetku donesena 12. srpnja 2016.)⁷⁰⁰, prijenosi su se mogli provoditi samo na temelju drugih pravnih osnova, poput standardnih ugovornih klauzula ili obvezujućih korporativnih pravila. Nekoliko društava, uključujući društvo Facebook Irska (protiv kojega je pokrenut predmet koji je doveo do poništavanja Odluke o „sigurnoj luci”), počelo je primjenjivati standardne ugovorne klauzule kako bi nastavili prenositi podatke između EU-a i SAD-a.

G. Schrems podnio je pritužbu irskom nadzornom tijelu, zatraživši da obustavi prijenose podataka u SAD na temelju standardnih ugovornih klauzula. U osnovi je tvrdio da prilikom prijenosa njegovih osobnih podataka iz irske podružnice društva Facebook društvu Facebook Inc., te na poslužitelje koji su smješteni u SAD-u, nije osigurana njihova zaštita. Društvo Facebook Inc. obvezano je zakonima SAD-a prema kojima bi moglo biti dužno otkriti osobne podatke tijelima za izvršavanje zakonodavstva u SAD-u, a europski građani nemaju na raspolaganju nikakav pravni lijek protiv takve prakse⁷⁰¹. Zbog toga je SEU zaključio da je Odluka o „sigurnoj luci” nevaljana, a iako je presuda Suda bila ograničena na preispitivanje te odluke, tužitelj je smatrao da su postavljena pitanja relevantna i za prijenos koji se temelji na ugovornim klauzulama. U trenutku izrade priručnika predmet je razmatrao irski Visoki sud. Čini se da tužitelj namjerava pokrenuti postupak pred SEU-om kako bi

698 Europska komisija (2010.), Odluka Komisije 2010/87/EU od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL 2010 L 39. U trenutku izrade priručnika upotreba standardnih ugovornih klauzula kao osnove za prijenose osobnih podataka u SAD bila je predmet sudskog postupka pred irskim Visokim sudom.

699 SEU, C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VV], 6. listopada 2015.

700 Provedbena odluka Komisije (EU) 2016/1250 od 12. srpnja 2016. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, SL L 207.

701 Više informacija potražite u [revidiranoj pritužbi](#) (dostupnoj na engleskom jeziku) protiv društva Facebook Ireland Ltd, koju je g. Maximilian Schrems podnio irskom Povjereniku za zaštitu podataka 1. prosinca 2015.

osporio valjanost odluke Europske komisije o standardnim ugovornim klauzulama. Kao što je opisano u [poglavlju 5.](#), samo SEU ima ovlast proglasiti neki instrument EU-a nevaljanim.

Prijenosi koji podliježu obvezujućim korporativnim pravilima

Pravom EU-a dopuštaju se i prijenosi osobnih podataka na temelju obvezujućih korporativnih pravila za međunarodne prijenose koji se odvijaju unutar iste skupine poduzeća ili poduzeća koja se bave zajedničkom gospodarskom djelatnošću⁷⁰². Prije nego što se obvezujuća korporativna pravila mogu primijeniti kao sredstvo prijenosa osobnih podataka, nadležno nadzorno tijelo mora ih odobriti u skladu s obvezujućim korporativnim pravilima, služeći se mehanizmom konzistentnosti.

Da bi bila odobrena, obvezujuća korporativna pravila moraju biti pravno obvezujuća, obuhvaćati sva temeljna načela zaštite podataka te se moraju primjenjivati na sve članove skupine, koji su ih dužni provoditi. Njima se moraju izričito dodijeliti provediva prava ispitanicima, ona moraju uključivati sva temeljna načela zaštite podataka i biti u skladu s određenim službenim zahtjevima, poput navođenja strukture poduzeća, opisivanja prijenosa i načina primjene načela zaštite podataka. To uključuje pružanje odgovarajućih informacija ispitanicima. Obvezujućim korporativnim pravilima moraju se, među ostalim, utvrditi prava ispitanika i odredbe o odgovornosti za svako kršenje pravila⁷⁰³. Prilikom odobravanja obvezujućih korporativnih pravila aktivirat će se mehanizam konzistentnosti za suradnju nadzornih tijela (opisan u [poglavlju 5.](#)).

U okviru mehanizma konzistentnosti, vodeće nadzorno tijelo preispituje predložena obvezujuća korporativna pravila, donosi nacrt odluke i o tome obavješćuje EOZP. Odbor daje mišljenje o tom predmetu, a vodeće nadzorno tijelo može službeno odobriti obvezujuća korporativna pravila dok „što je više moguće uzima u obzir” mišljenje Odbora. To mišljenje nije pravno obvezujuće, no ako ga nadzorno tijelo namjerava zanemariti, aktivirat će se mehanizam za rješavanje sporova, a Odbor će trebati donijeti pravno obvezujuću odluku dvotrećinskom većinom članova⁷⁰⁴.

702 Opća uredba o zaštiti podataka, članak 47.

703 Detaljan opis dostupan je u Općoj uredbi o zaštiti podataka, članak 47.

704 *Ibid.*, članak 57. stavak 1. točka (s), članak 58. stavak 1. točka (j), članak 64. stavak 1. točka (f), članak 65. stavci 1. i 2.

Prema **pravu Vijeća Europe**, *ad hoc* ili standardizirane zaštitne mjere, koje su ugrađene u pravno obvezujući dokument⁷⁰⁵, također uključuju obvezujuća korporativna pravila.

7.3.3. Odstupanja za posebne situacije

Unutar prava EU-a prijenosi osobnih podataka u treće zemlje mogu biti opravdani čak i u nedostatku odgovarajuće odluke ili zaštitnih mjera, poput standardnih ugovornih klauzula ili obvezujućih korporativnih pravila, u bilo kojem od sljedećih slučajeva:

- ispitanik izričito pristaje na prijenos podataka,
- ispitanik sklapa ili se priprema sklopiti ugovorni odnos u sklopu kojega je nužan prijenos podataka u inozemstvo,
- sklapanje ugovora između voditelja obrade podataka i treće strane u interesu ispitanika,
- važni razlozi javnog interesa,
- postavljanje, ostvarivanje ili obrana pravnih zahtjeva,
- zaštita životno važnih interesa ispitanika,
- prijenos podataka iz javnih registara (radi se o prevladavajućim interesima javnosti koji se tiču pristupa informacijama pohranjenima u javnim registrima)⁷⁰⁶.

Ako se ne primjenjuje nijedan od ovih uvjeta, a prijenosi se ne mogu temeljiti na odluci o primjerenosti ili odgovarajućim zaštitnim mjerama, prijenos se može ostvariti samo ako se ne ponavlja, ako se odnosi samo na ograničen broj ispitanika te je nužan za potrebe uvjerljivih, legitimnih interesa voditelja obrade podataka, pod uvjetom da oni nisu podređeni pravima ispitanika⁷⁰⁷. U tim slučajevima voditelj obrade mora procijeniti okolnosti prijenosa i odrediti zaštitne mjere. Također mora

⁷⁰⁵ Modernizirana Konvencija br. 108, članak 14. stavak 3. točka (b).

⁷⁰⁶ Opća uredba o zaštiti podataka, članak 49.

⁷⁰⁷ *Ibid.*

obavijestiti nadzorno tijelo i dotične ispitanike o prijenosu i o legitimnim interesima kojima ga opravdava.

Činjenica da su odstupanja krajnja mjera za zakonite prijenose⁷⁰⁸ (koja se primjenjuje samo u slučaju nedostatka odluke o primjerenosti i drugih zaštitnih mjera) pokazuje koliko su ona iznimna, a dodatno je naglašena u uvodnim izjavama OUZP-a⁷⁰⁹. Stoga se odstupanja prihvaćaju kao mogućnost „prijenosa u određenim okolnostima” na temelju privole i kada je „prijenos povremen i nužan”⁷¹⁰ s obzirom na ugovor ili pravni zahtjev.

Usto, sukladno smjernicama Radne skupine iz članka 29., oslanjanje na odstupanja za posebne situacije mora biti izuzetak, temeljiti se na pojedinačnim slučajevima i ne smije se primjenjivati za masovne ili ponavljajuće prijenose⁷¹¹. Europski nadzor-
nik za zaštitu podataka također je naglasio da odstupanja trebaju biti izuzetak kada se primjenjuju kao pravna osnova za prijenose na temelju Uredbe (EZ) br. 45/2001, napominjući da se to rješenje treba primjenjivati „u ograničenim slučajevima” i „za povremene prijenose”⁷¹².

Primjer: Društvo koje pruža usluge globalnog distribucijskog sustava (GDS), sa sjedištem u SAD-u, stavlja na raspolaganje mrežni sustav za rezervacije većem broju zrakoplovnih kompanija, hotela i brodova za krstarenje diljem svijeta te obrađuje podatke za desetke milijuna osoba u EU-u. Za prvotni prijenos podataka na njegove poslužitelje u SAD-u društvo koje pruža GDS oslanja se na odstupanje kao zakonitu osnovu za prijenose, odnosno na nužnost sklapanja ugovora. Stoga se ne poziva ni na kakve druge zaštitne mjere za osobne podatke koji potječu iz Europe, prenose se u SAD i zatim distribuiraju hotelima diljem svijeta (što znači da nema zaštitnih mjera ni za daljnje prijenose). Društvo koje pruža GDS ne pridržava se zahtjeva iz OUZP-a za zakonite međunarodne prijenose podataka jer se oslanja na odstupanje kao zakonitu osnovu za masovne prijenose.

708 *Ibid.*, članak 49. stavak 1.

709 *Ibid.*, članak 49. stavak 1. točke (a), (b) i (e) i uvodnu izjavu 113.

710 *Ibid.*, članak 49. stavak 1.

711 Radna skupina iz članka 29. (2005.), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 114, Bruxelles, 25. studenoga 2005.

712 Europski nadzor-
nik za zaštitu podataka, The transfer of personal data to third countries and international organisations by EU institutions and bodies (Prijenos osobnih podataka u treće zemlje ili međunarodne organizacije koji vrše institucije i tijela EU-a), Dokument o stajalištu, Bruxelles, 14. srpnja 2014., str. 15.

Ako odluka o primjerenosti nije donesena, EU ili njegove države članice smiju utvrditi ograničenja prijenosa pojedinih kategorija osobnih podataka trećoj zemlji, unatoč ispunjavanju drugih uvjeta za takve prijenose, iz razloga javnog interesa. Takva se ograničenja trebaju smatrati iznimkama, a države članice moraju u odgovarajućim odredbama obavijestiti Komisiju⁷¹³.

Pravom Vijeća Europe dopušta se prijenos podataka na područja koja nemaju odgovarajuću zaštitu podataka u sljedećim slučajevima:

- ispitanik je dao privolu,
- interesi ispitanika uvjetuju takav prijenos,
- prisutni su prevladavajući legitimni interesi, posebice važni javni interesi, propisani zakonom,
- to je nužna i razmjerna mjera u demokratskom društvu⁷¹⁴.

7.3.4. Prijenosi koji se temelje na međunarodnim sporazumima

EU može sklapati međunarodne sporazume s trećim zemljama kojima se uređuje prijenos osobnih podataka u posebne svrhe. Ti sporazumi moraju sadržavati odgovarajuće zaštitne mjere kako bi se osigurala zaštita osobnih podataka dotičnih pojedinaca. OUZP-om se ne dovode u pitanje ti međunarodni sporazumi⁷¹⁵.

Države članice mogu također sklopiti međunarodne sporazume s trećim zemljama ili međunarodnim organizacijama koje osiguravaju odgovarajuću razinu zaštite temeljnih prava i sloboda pojedinaca, u mjeri u kojoj ti sporazumi ne utječu na primjenu OUZP-a.

Slično je pravilo propisano člankom 12. stavkom 3. točkom (a) modernizirane Konvencije br. 108.

⁷¹³ Vidjeti Opću uredbu o zaštiti podataka, članak 49. stavak 5.

⁷¹⁴ Modernizirana Konvencija br. 108, članak 14. stavak 4.

⁷¹⁵ Opća uredba o zaštiti podataka, uvodna izjava 102.

Primjeri međunarodnih sporazuma koji se odnose na prijenos osobnih podataka sporazumi su o evidencijama podataka o putnicima (PNR).

Evidencija podataka o putnicima

Zrakoplovne kompanije u postupku rezervacije letova prikupljaju podatke iz evidencije podataka o putnicima koji, među ostalim, uključuju imena, adrese, podatke o kreditnoj kartici te brojeve sjedala putnika. Zrakoplovne kompanije prikupljaju te podatke i za vlastite komercijalne potrebe. Europska unija sklopila je sporazume s određenim trećim zemljama (Australijom, Kanadom i SAD-om) o prijenosu podataka iz evidencije podataka o putnicima radi sprečavanja, otkrivanja, istrage i progona terorističkih činova ili ozbiljnog transnacionalnog kriminala. Unija je 2016. također donijela Direktivu (EU) 2016/861, poznatu i kao Direktiva EU-a o evidenciji podataka o putnicima⁷¹⁶. Tom se Direktivom utvrđuje pravni okvir za države članice EU-a koji se odnosi na prijenos podataka iz evidencija podataka o putnicima nadležnim tijelima u trećim zemljama, također kako bi se spriječili, otkrili, istraživali ili progonili teroristički činovi i ozbiljna kaznena djela. Prijenosi podataka iz evidencija nadležnim tijelima trećih zemalja razlikuju se ovisno o slučaju i podliježu pojedinačnoj procjeni nužnosti prijenosa za svrhe navedene u Direktivi i poštovanju temeljnih prava.

Usklađenost sporazuma o evidencijama podataka o putnicima između EU-a i trećih zemalja s temeljnim pravima na privatnost i zaštitu podataka koja su zajamčena Poveljom EU-a o temeljnim pravima dovela se u pitanje u prošlosti. Kada je EU nakon pregovora s Kanadom 2014. potpisao sporazum o prijenosu i obradi podataka iz evidencije podataka o putnicima, Europski parlament odlučio je SEU-u prosljediti predmet procjene zakonitosti sporazuma s pravom EU-a, posebice s obzirom na članke 7. i 8. Povelje.

Primjer: U Mišljenju o zakonitosti sporazuma o evidenciji podataka o putnicima između EU-a i Kanade⁷¹⁷ SEU je smatrao da predviđeni sporazum u tadašnjem obliku nije usklađen s temeljnim pravima koja su zajamčena Poveljom te se stoga ne može sklopiti. Budući da je uključivao obradu osobnih podataka, predstavljao je miješanje u pravo na zaštitu osobnih podataka

⁷¹⁶ Direktiva (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela, SL 2016 L 119.

⁷¹⁷ SEU, *Mišljenje 1/15 Suda* [VV], 26. srpnja 2017.

koje je zajamčeno člankom 8. Povelje. Istodobno je predstavljao i ograničenje prava na poštovanje privatnog života, utvrđeno u članku 7., jer se, gledano u cjelini, podaci iz evidencije imena putnika mogu grupirati i analizirati na način koji bi otkrio putne navike, odnose među pojedincima, informacije o njihovu financijskom statusu, prehrambene navike i zdravstveno stanje, čime bi se umiješalo u privatne živote pojedinaca.

Miješanje u temeljna prava koje bi predviđeni sporazum uzrokovao odnosilo se na cilj od općeg interesa, točnije javnu sigurnost i borbu protiv terorizma i ozbiljnog transnacionalnog kriminala. Međutim, SEU je podsjetio da takvo miješanje mora biti ograničeno na ono što je strogo nužno za postizanje predviđenog cilja da bi bilo opravdano. Nakon preispitivanja odredbi predviđenog sporazuma, SEU je zaključio da ne ispunjava kriterij „strogo nužnog”. Među ostalim, u donošenju tog zaključka SEU je razmatrao sljedeće čimbenike:

- činjenicu da je predviđeni sporazum podrazumijevao prijenos osjetljivih podataka. Podaci iz evidencije podataka o putnicima, prikupljeni sukladno predviđenom sporazumu, mogli su uključivati osjetljive podatke koji otkrivaju rasno ili etničko podrijetlo, vjerska uvjerenja ili zdravstveno stanje putnika. Prijenos i obrada osjetljivih podataka, koje su vršila kanadska nadležna tijela, mogli su predstavljati rizik za nediskriminacijsko načelo te su stoga zahtijevali precizno i uvjerljivo opravdanje na temelju osnove koja nije javna sigurnost ili borba protiv ozbiljnog kriminala. Predviđeni sporazum nije pružio takvo opravdanje⁷¹⁸,
- Sud je smatrao da neprekidna pohrana podataka iz evidencije podataka o putnicima tijekom razdoblja od pet godina, čak i nakon odlaska putnika iz Kanade, također prelazi granice strogo nužnog. SEU je smatrao da bi se kanadskim nadležnim tijelima moglo dopustiti zadržavanje podataka o putnicima za koje objektivni dokazi ukazuju da bi mogli predstavljati prijetnju javnoj sigurnosti, čak i nakon što te osobe napuste Kanadu. No, pohrana osobnih podataka *svih* putnika, za koje ne postoje čak ni neizravni dokazi da predstavljaju prijetnju javnoj sigurnosti, nije bila opravdana⁷¹⁹.

⁷¹⁸ *Ibid.*, t. 165.

⁷¹⁹ *Ibid.*, t. od 204. do 207.

Savjetodavni odbor Konvencije br. 108 dao je mišljenje o implikacijama sporazuma o evidencijama podataka o putnicima za zaštitu podataka na temelju prava Vijeća Europe⁷²⁰.

Podaci o porukama

Belgijsko Društvo za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT), koje obrađuje većinu globalnih prijenosa novca iz europskih banaka, poslovalo je putem „zrcalnog“ centra u SAD-u te je zaprimilo zahtjev za otkrivanje podataka Ministarstvu financija SAD-a u svrhu istrage terorizma u sklopu njegova Programa za praćenje financiranja terorizma⁷²¹.

S gledišta EU-a, nije postojala primjerena pravna osnova za otkrivanje tih podataka, koji su se uglavnom odnosili na građane EU-a, u SAD-u samo zato što je ondje bio smješten jedan od SWIFT-ovih centara za obradu podataka.

Poseban sporazum između EU-a i SAD-a, poznat kao Sporazum o SWIFT-u, sklopljen je 2010. godine kako bi se osigurala potrebna pravna osnova i odgovarajući standardi zaštite podataka⁷²².

Prema tom sporazumu, financijski podaci koje pohranjuje SWIFT i dalje se dostavljaju Ministarstvu financija SAD-a u svrhu sprečavanja, istrage, otkrivanja ili progona terorizma ili financiranja terorističkih aktivnosti. Ministarstvo financija SAD-a može od SWIFT-a zatražiti financijske podatke pod uvjetom:

- da su financijski podaci u zahtjevu što jasnije utvrđeni,

720 Vijeće Europe, Opinion on the Data protection implications of the processing of Passenger Name Records (Mišljenje o implikacijama obrade evidencija imena putnika za zaštitu podataka), T-PD(2016)18rev, 19. kolovoza 2016.

721 U tom kontekstu vidjeti: Radna skupina iz članka 29. (2011.), *Mišljenje 14/2011 o pitanjima zaštite podataka povezanim sa sprečavanjem pranja novca i financiranja terorizma*, WP 186, Bruxelles, 13. lipnja 2011.; Radna skupina iz članka 29. (2006.), *Mišljenje 10/2006 o obradi osobnih podataka koju provodi Društvo za svjetsku međubankovnu financijsku telekomunikaciju (SWIFT)*, WP 128, Bruxelles, 22. studenoga 2006.; belgijska Komisija za zaštitu privatnosti (*Commission de la protection de la vie privée*) (2008.), „Postupak kontrole i preporuke pokrenut spram društva SWIFT srl“, Odluka, 9. prosinca 2008.

722 Odluka Vijeća 2010/412/EU od 13. srpnja 2010. o sklapanju Sporazuma između Europske unije i Sjedinjenih Američkih Država o obradi i slanju podataka o izvješćima u vezi s financijskim plaćanjima iz Europske unije Sjedinjenim Američkim Državama za potrebe Programa za praćenje financiranja terorističkih djelatnosti, SL 2010 L 195, str. 3. i 4. Tekst Sporazuma priložen je toj odluci, SL 2010 L 195, str. 5.–14.

- da je u zahtjevu jasno potkrijepljena nužnost podataka,
- da je zahtjev što precizniji kako bi se smanjila količina zatraženih podataka,
- da se u zahtjevu ne traže podaci koji se odnose na Jedinstveno područje plaćanja u eurima (SEPA)⁷²³.

Europol mora primiti primjerak svakog zahtjeva Ministarstva financija SAD-a i potvrditi poštuju li se načela Sporazuma o SWIFT-u⁷²⁴. Ako se potvrdi da se poštuju, SWIFT mora financijske podatke dostaviti izravno Ministarstvu financija SAD-a. Ministarstvo mora pohraniti financijske podatke u sigurnom fizičkom okruženju tako da im mogu pristupiti samo analitičari koji istražuju terorizam ili njegovo financiranje, a financijski podaci ne smiju biti međusobno povezani ni sa kojom drugom bazom podataka. Općenito se financijski podaci primljeni od SWIFT-a moraju izbrisati najkasnije pet godina od primitka. Financijski podaci koji su bitni za određene istrage ili progone mogu se zadržati sve dok su nužni za te istrage ili progone.

Ministarstvo financija SAD-a može prenijeti informacije iz podataka primljenih od SWIFT-a određenim tijelima policije, javne sigurnosti ili suzbijanja terorizma, unutar ili izvan SAD-a, isključivo radi istrage, otkrivanja, sprečavanja ili progona terorizma i njegova financiranja. Ako daljnji prijenos financijskih podataka uključuje građanina ili stanovnika države članice Europske unije, svaka razmjena podataka s tijelima treće zemlje podliježe prethodnoj privoli nadležnih tijela predmetne države članice. Mogu se napraviti izuzeća ako je razmjena podataka nužna za sprečavanje izravne i ozbiljne prijetnje javnoj sigurnosti.

Neovisna tijela koja provode nadzor, uključujući osobu koju imenuje Europska komisija, nadziru sukladnost s načelima Sporazuma o SWIFT-u. Ona mogu u stvarnom vremenu i retroaktivno pregledati sve pretrage pruženih podataka, zatražiti dodatne informacije za opravdanje poveznice tih pretraga s terorizmom te blokirati bilo koje ili sve pretrage kojima se krše zaštitne mjere utvrđene Sporazumom.

Ispitanici imaju pravo dobiti potvrdu nadležnog nadzornog tijela EU-a za zaštitu podataka da se poštuju njihova prava na zaštitu podataka. Ispitanici također imaju pravo na ispravak, brisanje ili blokiranje svojih podataka koje je prikupilo i pohranilo Ministarstvo financija SAD-a sukladno Sporazumu o SWIFT-u. Međutim, prava

⁷²³ *Ibid.*, članak 4. stavak 2.

⁷²⁴ Zajedničko nadzorno tijelo Europolu provelo je revizije Europolovih aktivnosti u tom području.

na pristup ispitanika mogu podlijevati određenim pravnim ograničenjima. Ako mu je pristup odbijen, ispitanika treba pisanim putem obavijestiti o odbijanju i o njegovu pravu na pravni lijek u vidu upravnog i sudskog postupka u SAD-u.

Sporazum o SWIFT-u vrijedi pet godina, a prvo razdoblje valjanosti trajalo je do kolovoza 2015. Automatski se produljuje na razdoblje od još jedne godine, osim ako jedna od stranaka obavijesti drugu najmanje šest mjeseci unaprijed o svojoj namjeri da ne produlji sporazum. Automatsko produljenje obavljeno je u kolovozu 2015., 2016. i 2017., a njime se osigurava valjanost Sporazuma o SWIFT-u barem do kolovoza 2018.⁷²⁵

725 *Ibid.*, članak 23. stavak 2.

8

Zaštita podataka u kontekstu policije i kaznenog pravosuđa

EU	Obuhvaćena pitanja	Vijeće Europe
Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa	Općenito	Modernizirana Konvencija br. 108
	Policija	<i>Police Recommendation</i> (Preporuka o policiji) <i>Practical Guide on the use of personal data in the police sector</i> (Praktični vodič o upotrebi osobnih podataka u sektoru policije)
	Nadzor	ESLJP, <i>B. B. protiv Francuske</i> , br. 5335/06, 2009. ESLJP, <i>S. i Harper protiv Ujedinjene Kraljevine [VV]</i> , br. 30562/04 i 30566/04, 2008. ESLJP, <i>Allan protiv Ujedinjene Kraljevine</i> , br. 48539/99, 2002. ESLJP, <i>Malone protiv Ujedinjene Kraljevine</i> , br. 8691/79, 1984. ESLJP, <i>Klass i drugi protiv Njemačke</i> , br. 5029/71, 1978. ESLJP, <i>Szabó i Vissy protiv Mađarske</i> , br. 37138/14, 2016. ESLJP, <i>Vetter protiv Francuske</i> , br. 59842/00, 2005.

EU	Obuhvaćena pitanja	Vijeće Europe
	Kibernetički kriminal	<i>Cybercrime Convention</i> (Konvencija o kibernetičkom kriminalu)
Ostali specifični pravni instrumenti		
Prümska odluka	Za posebne podatke: otiske prstiju, DNK, huliganstvo, podatke o putnicima u zračnom prometu, telekomunikacijske podatke itd.	Modernizirana Konvencija br. 108, članak 6. Preporuka o policiji, <i>Practical Guide on the use of personal data in the police sector</i> (Praktični vodič o upotrebi osobnih podataka u sektoru policije)
Švedska inicijativa (Okvirna odluka Vijeća 2006/960/PUP)	Pojednostavljene razmjene informacija i obavještajnih podataka među tijelima za izvršavanje zakonodavstva	ESLJP, <i>S. i Harper protiv Ujedinjene Kraljevine</i> [VV], br. 30562/04 i 30566/04, 2008.
Direktiva (EU) 2016/681 o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela SEU, spojeni predmeti C-293/12 i C-594/12, <i>Digital Rights Ireland i Kärntner Landesregierung i dr.</i> [VV], 2014. SEU, spojeni predmeti C-203/15 i C-698/15, <i>Tele2 Sverige i Home Department protiv Toma Watsona i dr.</i> [VV], 2016.	Zadržavanje osobnih podataka	ESLJP, <i>B. B. protiv Francuske</i> , br. 5335/06, 2009.
Uredba o Europolu Odluka o Eurojustu	Posebne agencije	Preporuka o policiji
Odluka o Schengenskom informacijskom sustavu II Uredba o VIS-u Uredba o Eurodacu CIS Decision (Odluka o CIS-u)	Posebni zajednički informacijski sustavi	Preporuka o policiji ESLJP, <i>Dalea protiv Francuske</i> , br. 964/07, 2010.

Radi uravnoteženja interesa pojedinca u pogledu zaštite podataka i interesa društva u pogledu prikupljanja podataka radi suzbijanja zločina i osiguravanja nacionalne i javne sigurnosti, Vijeće Europe i Europska unija donijeli su posebne pravne instrumente. U ovom dijelu pruža se pregled prava Vijeća Europe (dio 8.1.) i EU-a (dio 8.2.) koje se odnosi na zaštitu podataka u poslovima policije i kaznenog pravosuđa.

8.1. Pravo Vijeća Europe u području zaštite podataka, nacionalne sigurnosti, policije i kaznenog pravosuđa

Ključne točke

- Modernizirana Konvencija br. 108 i Preporuka o policiji Vijeća Europe odnose se na zaštitu podataka u svim područjima djelovanja policije.
- Konvencija o kibernetičkom kriminalu (Budimpeštanska konvencija) obvezujući je međunarodni pravni instrument koji se odnosi na kaznena djela počinjena nad elektroničkim mrežama i putem njih. Također je važna za istragu nekibernetičkih kaznenih djela koja uključuju elektroničke uređaje.

Jedna je značajna razlika između prava Vijeća Europe i EU-a ta što se **pravo Vijeća Europe** primjenjuje i na područje nacionalne sigurnosti. To znači da se ugovorne stranke moraju pridržavati područja primjene članka 8. EKLJP-a čak i u aktivnostima povezanim s nacionalnom sigurnošću. Nekoliko presuda ESLJP-a odnosilo se na državne aktivnosti u osjetljivim područjima zakonodavstva i prakse u vezi s nacionalnom sigurnošću⁷²⁶.

U pogledu policije i kaznenog pravosuđa na europskoj razini, moderniziranom Konvencijom br. 108 obuhvaćena su sva područja obrade osobnih podataka, a svrha je njezinih odredbi općenito urediti obradu osobnih podataka. Stoga se modernizirana Konvencija br. 108 odnosi na zaštitu podataka u području policije i kaznenog pravosuđa. Obrada genetskih podataka, osobnih podataka povezanih s kaznenim djelima, kaznenim postupcima i osudama te svim povezanim sigurnosnim mjerama, biometrijskih podataka koji služe za identifikaciju osobe te svih osjetljivih osobnih podataka

⁷²⁶ Vidjeti, primjerice, ESLJP, *Klass i drugi protiv Njemačke*, br. 5029/71, 6. rujna 1978.; ESLJP, *Rotaru protiv Rumunjske* [VV], br. 28341/95, 4. svibnja 2000. i ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. siječnja 2016.

dopuštena je samo kada su uspostavljene odgovarajuće zaštitne mjere protiv rizika koje obrada takvih podataka može uzrokovati za interese, prava i temeljne slobode ispitanika, a ponajviše rizika od diskriminacije⁷²⁷.

Pravne zadaće policije i tijela kaznenog pravosuđa često zahtijevaju obradu osobnih podataka koja može imati ozbiljne posljedice za dotične pojedince. Preporuka o policiji koju je Vijeće Europe donijelo 1987. pruža državama članicama Vijeća Europe smjernice o načinu provedbe načela Konvencije br. 108 u kontekstu obrade osobnih podataka koju provode policijska tijela⁷²⁸. Preporuka je dopunjena praktičnim vodičem o upotrebi osobnih podataka u sektoru policije, koji je donio Savjetodavni odbor Konvencije br. 108⁷²⁹.

Primjer: U predmetu *D. L. protiv Bugarske*⁷³⁰ socijalna služba smjestila je tužitelja u zaštićenu obrazovnu ustanovu sukladno sudskom nalogu. Sva pisana korespondencija i telefonski razgovori podvrgnuti su općem i neselektivnom nadzoru ustanove. ESLJP je smatrao da je prekršen članak 8. jer dotična mjera nije bila nužna u demokratskom društvu. ESLJP je naveo da se mora poduzeti sve što je moguće kako bi se maloljetnicima smještenima u ustanovu omogućio dostatan kontakt s vanjskim svijetom jer je to neophodno za njihovo pravo na ophođenje s dostojanstvom i od ključne važnosti za pripremu njihove ponovne integracije u društvo. To se podjednako odnosilo na posjete i na pisanu korespondenciju ili telefonske razgovore. Nadalje, u provođenju nadzora nije se pravila razlika između komunikacije s članovima obitelji i komunikacije s NVO-ima koji zastupaju prava djece ili odvjetnicima. Osim toga, odluka o presretanju komunikacije nije bila utemeljena na pojedinačnoj analizi rizika u svakom pojedinom slučaju.

Primjer: U predmetu *Dragojević protiv Hrvatske*⁷³¹ tužitelj je bio osumnjičen za krijumčarenje droge. Proglašen je krivim nakon što je istražni sudac odobrio primjenu mjera tajnog nadzora kako bi se presreli njegovi telefonski pozivi. ESLJP je smatrao da je ta mjera, protiv koje je podnesena pritužba,

727 Modernizirana Konvencija br. 108, članak 6.

728 Vijeće Europe, Odbor ministara (1987.), Preporuka Rec(87)15 državama članicama o uporabi osobnih podataka u policijskom sektoru, 17. rujna 1987.

729 Vijeće Europe (2018.), Savjetodavni odbor Konvencije br. 108, *Practical Guide on the use of personal data in the police sector* (Praktični vodič o upotrebi osobnih podataka u sektoru policije), T-PD(2018)1.

730 ESLJP, *D. L. protiv Bugarske*, br. 7472/14, 19. svibnja 2016.

731 ESLJP, *Dragojević protiv Hrvatske*, br. 68955/11, 15. siječnja 2015.

predstavljala miješanje u pravo na poštovanje privatnog života i dopisivanja. Odobrenje istražnog suca temeljilo se isključivo na izjavi tužiteljstva da se „istraga nije mogla provesti drugim sredstvima”. ESLJP je također istaknuo da su kazneni sudovi ograničili svoju procjenu o primjeni mjera nadzora te da vlada nije iznijela dostupne pravne lijekove. Stoga je prekršen članak 8.

8.1.1. Preporuka o policiji

Ustaljeni je stav ESLJP-a da pohrana i zadržavanje osobnih podataka od strane policijskih ili tijela nacionalne sigurnosti predstavlja miješanje u članak 8. stavak 1. Europske konvencije o ljudskim pravima. Mnoge se presude ESLJP-a odnose na obražloženje takvih miješanja⁷³².

Primjer: U predmetu *B. B. protiv Francuske*⁷³³ tužitelj je osuđen na zatvorsku kaznu za kaznena djela seksualnog zlostavljanja maloljetnika u dobi od 15 godina kao osoba na položaju povjerenja. Odslužio je zatvorsku kaznu 2000. Nakon godinu dana zatražio je da se navod o zatvorskoj kazni ukloni iz njegove kaznene evidencije, no taj je zahtjev odbijen. Francuskim zakonom iz 2004. uspostavljena je nacionalna pravosudna baza podataka seksualnih prijestupnika i tužitelj je obaviješten o tome da je uvršten u nju. ESLJP je zaključio da uvrštavanje osuđenog seksualnog prijestupnika u nacionalnu pravosudnu bazu podataka potpada pod članak 8. Europske konvencije o ljudskim pravima. Međutim, budući da su uvedene dostatne mjere za zaštitu podataka, kao što je pravo ispitanika da zatraži brisanje podataka, ograničeno trajanje pohrane podataka i ograničen pristup takvim podacima, postignuta je dobra ravnoteža između sukobljenih privatnih i javnih interesa. ESLJP je stoga zaključio da nije došlo do kršenja članka 8. Konvencije.

Primjer: U predmetu *S. i Marper protiv Ujedinjene Kraljevine*⁷³⁴ oba su tužitelja optužena, ali ne i osuđena, za kaznena djela. Međutim, policija je ipak zadržala i pohranila njihove otiske prstiju, stanične uzorke i profile DNK-a. Neograničeno zadržavanje navedenih biometrijskih podataka bilo je dopušteno

732 Vidjeti, primjerice, ESLJP, *Leander protiv Švedske*, br. 9248/81, 26. ožujka 1987.; ESLJP, *M. M. protiv Ujedinjene Kraljevine*, br. 24029/07, 13. studenoga 2012.; ESLJP, *M. K. protiv Francuske*, br. 19522/09, 18. travnja 2013. ili ESLJP, *Aycaguer protiv Francuske*, br. 8806/12, 22. lipnja 2017.

733 ESLJP, *B. B. protiv Francuske*, br. 5335/06, 17. prosinca 2009.

734 ESLJP, *S. i Marper protiv Ujedinjene Kraljevine* [VV], br. 30562/04 i 30566/04, 4. prosinca 2008., t. 119. i 125.

zakonom ako je osoba bila osumnjičena za kazneno djelo, čak i ako je osumnjičenik kasnije oslobođen od optužbi ili pušten na slobodu. ESLJP je smatrao da je sveobuhvatno i neselektivno zadržavanje osobnih podataka koje nije vremenski ograničeno i pri kojemu oslobođeni pojedinci imaju samo ograničene mogućnosti zatražiti brisanje predstavljalo nerazmjerno miješanje u prava tužitelja na poštovanje privatnog života. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Ključno pitanje u kontekstu elektroničkih komunikacija miješanje je javnih tijela u prava na privatnost i zaštitu podataka. Sredstva nadzora ili presretanje komunikacije, poput uređaja za prisluškivanje, dopušteni su samo ako je to propisano zakonom i ako predstavlja nužnu mjeru u demokratskom društvu zbog interesa:

- zaštite državne sigurnosti,
- javne sigurnosti,
- monetarnih interesa države,
- suzbijanja kaznenih djela, ili
- zaštite ispitanika ili prava i sloboda drugih osoba.

Mnoge druge presude ESLJP-a odnose se na obrazloženje miješanja u pravo na privatnost provođenjem nadzora.

Primjer: U predmetu *Allan protiv Ujedinjene Kraljevine*⁷³⁵ nadležna su tijela tajno snimala privatne razgovore zatvorenika s prijateljem u zatvorskom prostoru za posjete i sa suoptuženikom u zatvorskoj ćeliji. ESLJP je smatrao da je uporaba uređaja za audiosnimanje i videosnimanje u tužiteljevoj ćeliji, zatvorskom prostoru za posjete i na kolegi zatvoreniku predstavljala miješanje u tužiteljevo pravo na privatni život. Budući da nije postojao pravni sustav kojim bi se regulirala policijska uporaba tajnih uređaja za snimanje u danom trenutku, navedeno miješanje nije bilo u skladu sa zakonom. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

⁷³⁵ ESLJP, *Allan protiv Ujedinjene Kraljevine*, br. 48539/99, 5. studenoga 2002.

Primjer: U predmetu *Roman Zakharov protiv Rusije*⁷³⁶ tužitelj je pokrenuo sudski postupak protiv triju operatera mobilnih mreža. Tvrdio je da je prekršeno njegovo pravo na privatnost telefonske komunikacije jer su operateri postavili opremu koja je omogućila Saveznoj sigurnosnoj službi Ruske Federacije da presretne njegovu telefonsku komunikaciju bez prethodnog sudskog odobrenja. ESLJP je smatrao da nacionalne zakonske odredbe kojima se uređuje presretanje komunikacija ne pružaju odgovarajuća i djelotvorna jamstva protiv proizvoljnog postupanja i rizika od zlouporabe. Naime, nacionalnim zakonima nije bilo propisano brisanje pohranjenih podataka nakon ostvarenja svrhe pohrane. Nadalje, iako je bilo potrebno sudsko odobrenje, sudski nadzor bio je ograničen.

Primjer: U predmetu *Szabó i Vissy protiv Mađarske*⁷³⁷ tužitelji su tvrdili da se mađarskim zakonodavstvom krši članak 8. EKLJP-a jer zakonodavstvo nije dovoljno detaljno ni precizno. Također su tvrdili da se zakonodavstvom ne osiguravaju odgovarajuća jamstva protiv zlouporabe i proizvoljnog postupanja. ESLJP je smatrao da mađarskim zakonima nije propisano da nadzor podliježe odobrenju suda. Unatoč tome, ESLJP je napomenuo da iako je taj nadzor podlijegao odobrenju ministra pravosuđa, bio je političke naravi i njime se nije mogla osigurati potrebna procjena „stroge nužnosti“. Nadalje, nacionalnim zakonima nije propisano sudsko preispitivanje s obzirom na to da se dotičnim osobama ne bi poslala nikakva obavijest. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

Budući da obrada podataka koju provode policijske službe može znatno utjecati na osobe koje su njome zahvaćene, posebno su potrebna detaljna pravila zaštite podataka prilikom obrade osobnih podataka u tom području. Preporukom o policiji Vijeća Europe nastojalo se riješiti to pitanje pružanjem smjernica o načinu prikupljanja osobnih podataka za policijske poslove, načinu čuvanja podatkovnih datoteka u tom području, osobama koje smiju pristupiti tim datotekama, uključujući uvjete za prijenos osobnih podataka stranim policijskim tijelima, načinu na koji ispitanici trebaju imati mogućnost ostvarivanja svojih prava na zaštitu podataka te načinu provedbe kontrole neovisnih tijela. Također je razmotrena obveza pružanja odgovarajuće sigurnosti podataka.

736 ESLJP, *Roman Zakharov protiv Rusije* [VV], br. 47143/06, 4. prosinca 2015.

737 ESLJP, *Szabó i Vissy protiv Mađarske*, br. 37138/14, 12. siječnja 2016.

Preporukom se ne predviđa otvoreno, neselektivno prikupljanje osobnih podataka policijskih tijela. Njome se ograničava prikupljanje osobnih podataka koje provode policijska tijela na mjeru nužnu za sprečavanje stvarne opasnosti ili suzbijanje određenog kaznenog djela. Svako dodatno prikupljanje podataka trebalo bi se temeljiti na posebnom nacionalnom zakonodavstvu. Obrada osjetljivih podataka treba biti ograničena na mjeru koja je apsolutno nužna u kontekstu određene istrage.

Ako se osobni podaci prikupljaju bez znanja ispitanika, ispitanika se mora obavijestiti o prikupljanju podataka čim otkrivanje više ne ometa istragu. Prikupljanje podataka tehničkim nadzorom ili drugim automatiziranim sredstvima također se mora temeljiti na posebnoj pravnoj osnovi.

Primjer: U predmetu *Versini-Campinchi i Crasnianski protiv Francuske*⁷³⁸ tužiteljica, inače odvjetnica, telefonski je razgovarala s klijentom čija je telefonska linija prisluškivana na zahtjev istražnog suca. Transkript razgovora pokazao je da je ona otkrila informacije obuhvaćene odvjetničkom tajnom. Tužitelj je poslao te informacije odvjetničkoj komori, koja je tužiteljici izrekla novčanu kaznu. ESLJP je potvrdio da je došlo do miješanja u pravo na poštovanje privatnog života i dopisivanja, ne samo osobe čiji je telefon prisluškivan nego i tužiteljice čija je komunikacija presretana i transkribirana. Miješanje je provedeno u skladu sa zakonom i imalo je legitiman cilj sprečavanja narušavanja reda. Tužiteljica je ishodila preispitivanje zakonitosti podnošenja transkripta prisluškivanog telefonskog razgovora u kontekstu disciplinskog postupka koji se vodio protiv nje. Iako nije mogla podnijeti zahtjev za poništavanje transkripta telefonskog razgovora, ESLJP je smatrao da je postojao učinkovit nadzor kojim se sporno miješanje moglo ograničiti na ono što je nužno u demokratskom društvu. ESLJP je smatrao neučinkovitim argument da mogućnost kaznenog postupka protiv odvjetnika na temelju transkripta može imati negativan učinak na slobodu komunikacije između odvjetnika i njegova klijenta, a stoga i na prava na obranu tog klijenta, kada odvjetnično otkrivanje informacija može predstavljati protuzakonito postupanje s njezine strane. Stoga nije došlo do kršenja članka 8.

U Preporuci o policiji Vijeća Europe naveden je zaključak da se pri pohrani osobnih podataka mora jasno razlikovati administrativne podatke od policijskih podataka, osobne podatke različitih vrsta ispitanika, kao što su osumnjičenici, osuđenici, žrtve

⁷³⁸ ESLJP, *Versini-Campinchi i Crasnianski protiv Francuske*, br. 49176/11, 16. lipnja 2016.

i svjedoci te podatke koji se smatraju čvrstim činjenicama od onih koji se temelje na sumnjama ili nagađanjima.

Svrha u koju se policijski podaci mogu upotrijebiti mora biti strogo ograničena. To ima posljedice na otkrivanje policijskih podataka trećim stranama. Prijenos ili otkrivanje takvih podataka unutar policijskog sektora treba ovisiti o tome postoji li legitiman interes za dijeljenje informacija. Prijenos ili otkrivanje takvih podataka izvan policijskog sektora treba biti dopušteno samo ako postoji jasna pravna obveza ili ovlaštenje.

Primjer: U predmetu *Karabeyoğlu protiv Turske*⁷³⁹ telefonske linije tužitelja, inače suca, nadzirale su se u okviru kaznene istrage protuzakonite organizacije čiji je on navodno bio član ili kojoj je navodno pružao pomoć i potporu. Nakon donošenja odluke da neće podići tužbu, javni tužitelj zadužen za kaznenu istragu uništio je predmetne snimke. Međutim, primjerak je ostao u posjedu sudskih istražitelja koji su te materijale iskoristili u kontekstu disciplinske istrage protiv tužitelja. ESLJP je smatrao da je prekršeno mjerodavno zakonodavstvo jer su informacije upotrijebljene u svrhe u koje nisu prikupljene i nisu uništene unutar zakonskog roka. Miješanje u tužiteljevo pravo na poštovanje privatnog života nije bilo u skladu sa zakonom kad je bila riječ o disciplinskom postupku pokrenutom protiv njega.

Međunarodni prijenos ili otkrivanje podataka treba biti ograničeno na strana policijska tijela i temeljiti se na posebnim zakonskim odredbama, možda i međunarodnim sporazumima, osim ako je to nužno za sprečavanje ozbiljne i neizbježne opasnosti.

Obrada podataka koju vrši policija mora biti podvrgnuta neovisnom nadzoru kako bi se osigurala sukladnost s nacionalnim zakonodavstvom o zaštiti podataka. Ispitanici moraju imati sva prava na pristup utvrđena u moderniziranoj Konvenciji br. 108. Kada su prava ispitanika na pristup ograničena na temelju članka 9. Konvencije br. 108, u interesu učinkovitih policijskih istraga i izvršavanja kaznenopravnih sankcija, ispitanici moraju imati pravo žalbe nacionalnom nadzornom tijelu za zaštitu podataka ili drugom neovisnom tijelu sukladno nacionalnom zakonu.

⁷³⁹ ESLJP, *Karabeyoğlu protiv Turske*, br. 30083/10, 7. lipnja 2016.

8.1.2. Budimpeštanska konvencija o kibernetičkom kriminalu

Budući da se u kriminalnim aktivnostima sve češće rabe elektronički sustavi za obradu podataka, te one na njih utječu, potrebne su nove kaznenopravne odredbe kojima se rješava taj problem. Stoga je Vijeće Europe donijelo međunarodni pravni instrument, Konvenciju o kibernetičkom kriminalu, poznatu i kao Budimpeštanska konvencija, kao odgovor na problem kaznenih djela počinjenih nad elektroničkim mrežama i putem njih.⁷⁴⁰

Toj Konvenciji mogu pristupiti i države koje nisu članice Vijeća Europe. Do početka 2018. 14 država izvan Vijeća Europe⁷⁴¹ pristupilo je Konvenciji, a sedam drugih nečlanica pozvano je da se pridruži.

Konvencija o kibernetičkom kriminalu i dalje je najutjecajniji međunarodni sporazum koji se bavi kršenjima zakona putem [interneta](#) ili drugih [informacijskih mreža](#). Njezine stranke moraju ažurirati i uskladiti svoje kaznene zakone protiv [hakiranja](#) i ostalih povreda sigurnosti, uključujući [povrede autorskih prava](#), [računalno potpomognutu prijevaru](#), [dječju pornografiju](#) i druge zabranjene kibernetičke aktivnosti. Konvencijom su propisane i proceduralne ovlasti koje obuhvaćaju pretraživanje računalnih mreža i presretanje komunikacija u kontekstu suzbijanja kibernetičkog kriminala. Naposljetku, njome je omogućena učinkovita međunarodna suradnja. Dodatni protokol uz Konvenciju odnosi se na kriminalizaciju rasističke i ksenofobne propagande na računalnim mrežama.

Iako Konvencija zapravo nije instrument za promicanje zaštite podataka, njome se kriminaliziraju aktivnosti za koje je izgledno da će prekršiti prava ispitanika na zaštitu njegovih podataka. Sukladno Konvenciji, ugovorne stranke moraju donijeti zakonodavne mjere kojima će omogućiti nacionalnim tijelima da presretnu podatke o prometu i sadržaju⁷⁴². Njome se ugovorne stranke također obvezuju da pri provedbi Konvencije predvide odgovarajuću zaštitu ljudskih prava i sloboda, uključujući prava

740 Vijeće Europe, Odbor ministara (2001.), Konvencija o kibernetičkom kriminalu, CETS br. 185, Budimpešta, 23. studenoga 2001., stupila na snagu 1. srpnja 2004.

741 Australija, Kanada, Čile, Kolumbija, Dominikanska Republika, Izrael, Japan, Mauricijus, Panama, Senegal, Šri Lanka, Tonga, Tunis i Sjedinjene Američke Države. Pogledajte [Tablicu s potpisima i datumima ratifikacije Sporazuma br. 185, status u srpnju 2017.](#) (dostupno na engleskom jeziku).

742 Vijeće Europe, Odbor ministara (2001.), Konvencija o kibernetičkom kriminalu, CETS br. 185, Budimpešta, 23. studenoga 2001., članci 20. i 21.

zajamčena EKLJP-om, kao što je pravo na zaštitu podataka⁷⁴³. Ugovorne stranke ne moraju potpisati Konvenciju br. 108 da bi pristupile Budimpeštanskoj konvenciji o kibernetičkom kriminalu.

8.2. Pravo Unije o zaštiti podataka u području policije i kaznenog pravosuđa

Ključne točke

- Na razini Europske unije, zaštita podataka u policijskom i kaznenopravnom sektoru uređena je u kontekstu nacionalne i prekogranične obrade koju vrše policija i tijela kaznenog pravosuđa država članica i dionici EU-a.
- Na razini država članica Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa mora se ugraditi u nacionalno pravo.
- Posebnim pravnim instrumentima uređuje se zaštita podataka u prekograničnoj suradnji policije i tijela za izvršavanje zakonodavstva, posebice u području borbe protiv terorizma i prekograničnog kriminala.
- Za Agenciju Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol), Agenciju Europske unije za suradnju u kaznenom pravosuđu (Eurojust) te novoosnovani Ured europskog javnog tužitelja, tijela EU-a koja pomažu i promiču prekogranično izvršavanje zakonodavstva, postoje posebni propisi za zaštitu podataka.
- Posebni propisi za zaštitu podataka postoje i za zajedničke informacijske sustave uspostavljene na razini Europske unije za prekograničnu razmjenu informacija između nadležnih policijskih i pravosudnih tijela. Važni su primjeri Schengenski informacijski sustav II (SIS II), vizni informacijski sustav (VIS) i Eurodac, centralizirani sustav s podacima o otiscima prstiju državljana trećih zemalja i osoba bez državljanstva koji su podnijeli zahtjev za azil u jednoj od država članica EU-a.
- U tijeku je postupak ažuriranja navedenih odredbi o zaštiti podataka u EU-u, kako bi bile u skladu s odredbama Direktive o zaštiti podataka za policiju i tijela kaznenog pravosuđa.

⁷⁴³ *Ibid.*, članak 15. stavak 1.

8.2.1. Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa

Direktivom (EU) 2016/680 o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka (Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa)⁷⁴⁴ nastoji se zaštititi osobne podatke koji su prikupljeni i obrađeni u svrhe kaznenog prava, primjerice:

- sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje,
- izvršavanja kaznene sankcije, te
- u slučajevima kada policija ili druga tijela za izvršavanje zakonodavstva nastoje osigurati poštovanje zakona i zaštitu od prijetnji javnoj sigurnosti i temeljnim pravima društva koje mogu predstavljati kazneno djelo te spriječiti takve prijetnje.

Direktivom o zaštiti podataka za policiju i tijela kaznenog prava štite se osobni podaci različitih kategorija pojedinaca koji sudjeluju u kaznenim postupcima, poput svjedoka, doušnika, žrtvi, osumnjičenika i suučesnika. Policija i tijela kaznenog pravosuđa dužni su poštovati odredbe Direktive kad god obrađuju takve osobne podatke u svrhe izvršavanja zakonodavstva unutar osobnog i materijalnog područja primjene Direktive⁷⁴⁵.

Međutim, u određenim uvjetima dopuštena je i upotreba podataka u druge svrhe. Obrada podataka u svrhu izvršavanja zakonodavstva koja se razlikuje od one u koju su izvorno prikupljeni dopuštena je samo ako je to zakonito, nužno i proporcionalno na temelju nacionalnog prava ili prava Unije⁷⁴⁶. Na te druge svrhe primjenjuju se odredbe Opće uredbe o zaštiti podataka. Bilježenje i dokumentiranje dijeljenja

744 Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, SL 2016 L 119, str. 89. (Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa).

745 Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa, članak 2. stavak 1.

746 *Ibid.*, članak 4. stavak 2.

podataka jedna je od posebnih dužnosti nadležnih tijela radi pomaganja u pojašnjenju odgovornosti koje proizlaze iz pritužbi.

Nadležna tijela koja djeluju u području policije i kaznenog pravosuđa javna su tijela ili tijela koja su ovlaštena na temelju nacionalnog zakonodavstva i javnih ovlasti za obavljanje funkcija javnih tijela⁷⁴⁷, npr. privatni zatvori⁷⁴⁸. Područje primjene Direktive obuhvaća obradu podataka na nacionalnoj razini i prekograničnu obradu između policijskih i pravosudnih tijela država članica, kao i međunarodne prijenose koje nadležna tijela vrše prema trećim zemljama i međunarodnim organizacijama⁷⁴⁹. Ona ne obuhvaća nacionalnu sigurnost ni obradu osobnih podataka koju vrše institucije, tijela, uredi i agencije EU-a⁷⁵⁰.

Direktiva se uvelike temelji na načelima i definicijama iz Opće uredbe o zaštiti podataka, uzimajući u obzir posebnu prirodu područja policije i kaznenog pravosuđa. Nadzor mogu vršiti ista nadležna tijela države članice koja ga vrše i na temelju Opće uredbe o zaštiti podataka. Imenovanje službenika za zaštitu podataka i provođenje procjena učinka zaštite podataka uvedeni su u Direktivu kao nove obveze za policijska i tijela kaznenog pravosuđa⁷⁵¹. Iako su ti koncepti nadahnuti Općom uredbom o zaštiti podataka, Direktiva se odnosi na posebnu prirodu policijskih tijela i tijela kaznenog pravosuđa. U usporedbi s obradom podataka u komercijalne svrhe, koja je regulirana Uredbom, za obradu povezanu sa sigurnošću može biti potrebna određena razina fleksibilnosti. Primjerice, osiguravanje jednake razine zaštite ispitanika u pogledu prava na informacije te pristup vlastitim osobnim podacima ili njihovo brisanje, kao što je omogućena Općom uredbom o zaštiti podataka, moglo bi podrazumijevati da bi svaka radnja nadzora koja se provodi u svrhe izvršavanja zakonodavstva postala neučinkovita u kontekstu izvršavanja zakonodavstva. Direktiva stoga ne sadržava načelo transparentnosti. Na sličan se način i načela smanjenja količine podataka i ograničenja svrhe, prema kojima se osobni podaci moraju ograničiti na ono što je nužno za svrhe u koje se obrađuju te obrađivati u utvrđene i izričite svrhe, moraju fleksibilno primjenjivati u sklopu obrade u sigurnosne svrhe. Podaci koje

747 *Ibid.*, članak 3. stavak 7.

748 Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu na temelju članka 294. stavka 6. Ugovora o funkcioniranju Europske unije o stajalištu Vijeća o donošenju Direktive Europskog parlamenta i Vijeća o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija te slobodnom kretanju takvih podataka i o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, COM(2016) 213 final, Bruxelles, 11. travnja 2016.

749 Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa, poglavlje V.

750 *Ibid.*, članak 2. stavak 3.

751 *Ibid.*, članak 32. odnosno članak 27.

prikupе i pohrane nadležna tijela u određenom predmetu mogu se pokazati izuzetno korisnima u rješavanju budućih predmeta.

Načela povezana s obradom

U Direktivi o zaštiti podataka za policiju i tijela kaznenog pravosuđa utvrđuju se određene ključne zaštitne mjere u vezi s upotrebom osobnih podataka. Također se navode načela na kojima se temelji obrada tih podataka. Države članice moraju osigurati da su osobni podaci:

- obrađivani zakonito i pošteno,
- prikupljeni u posebne, izričite i zakonite svrhe te da ih se ne obrađuje na način koji nije u skladu s tim svrhama,
- primjereni i relevantni te da nisu pretjerani u odnosu na svrhe u koje se obrađuju,
- točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odgode izbrišu ili isprave,
- čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe u koje se osobni podaci obrađuju,
- obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera⁷⁵².

Sukladno Direktivi, obrada je zakonita samo u onoj mjeri u kojoj je nužna kako bi se obavila pojedina zadaća. Usto, to bi trebalo vršiti nadležno tijelo u svrhu ostvarenja ciljeva navedenih u Direktivi te bi se trebalo temeljiti na pravu Unije ili nacionalnom pravu⁷⁵³. Podaci se ne smiju čuvati dulje nego što je potrebno te se moraju izbrisati ili povremeno pregledavati unutar određenih vremenskih okvira. Smije ih upotrijebiti isključivo nadležno tijelo, i to u svrhu u koju su oni prikupljeni, preneseni ili stavljeni na raspolaganje.

⁷⁵² *Ibid.*, članak 4. stavak 1.

⁷⁵³ *Ibid.*, članak 8.

Prava ispitanika

Direktivom se također utvrđuju prava ispitanika. Ona uključuju sljedeće:

- pravo na informacije. Države članice moraju propisati obvezu voditelju obrade podataka da ispitaniku na raspolaganje stavi: 1) identitet i kontaktne podatke voditelja obrade, 2) kontaktne podatke službenika za zaštitu podataka, 3) svrhe predviđene obrade, 4) pravo na podnošenje pritužbe nadzornom tijelu i kontaktne podatke nadzornog tijela te 5) pravo na pristup osobnim podacima, njihov ispravak ili brisanje, ili ograničavanje obrade podataka⁷⁵⁴. Uz te opće zahtjeve za informacije, Direktivom se utvrđuje da u određenim slučajevima, kako bi se ispitanicima omogućilo ostvarivanje njihovih prava, voditelji obrade moraju pružiti informacije o pravnoj osnovi obrade i o razdoblju pohrane podataka. Ako će se osobni podaci prenositi drugim primateljima, uključujući treće zemlje ili međunarodne organizacije, ispitanici moraju biti obaviješteni o kategorijama takvih primatelja. Naposljetku, voditelji obrade moraju pružiti sve dodatne informacije, uzimajući u obzir posebne okolnosti u kojima se podaci obrađuju, primjerice slučajeve prikupljanja osobnih podataka u sklopu tajnog nadzora, odnosno bez znanja ispitanika. Time se jamči poštena obrada za ispitanika⁷⁵⁵,
- pravo na pristup osobnim podacima. Države članice moraju osigurati da ispitanik uživa pravo da zna obrađuju li se njegovi osobni podaci. Ako se oni obrađuju, ispitanik treba imati pristup određenim informacijama, kao što su kategorije podataka koji se obrađuju⁷⁵⁶. Međutim, to se pravo može ograničiti, primjerice kako bi se izbjeglo ometanje istrage ili dovođenje u pitanje progona kaznenih djela ili kako bi se zaštitila javna sigurnost te prava i slobode drugih⁷⁵⁷,
- pravo na ispravak osobnih podataka. Države članice dužne su osigurati da ispitanik bez nepotrebne odgode može ispravak netočnih osobnih podataka. Nadalje, ispitanik također ima pravo dopuniti nepotpune osobne podatke⁷⁵⁸,
- pravo na brisanje osobnih podataka i ograničavanje obrade. U određenim slučajevima voditelj obrade mora izbrisati osobne podatke. Nadalje, ispitanik može

754 *Ibid.*, članak 13. stavak 1.

755 *Ibid.*, članak 13. stavak 2.

756 *Ibid.*, članak 14.

757 *Ibid.*, članak 15.

758 *Ibid.*, članak 16. stavak 1.

osigurati brisanje svojih osobnih podataka, no samo kada se oni nezakonito obrađuju⁷⁵⁹. U određenim situacijama može se ograničiti obrada osobnih podataka umjesto brisanja podataka. To se može dogoditi 1) kada se osporava točnost osobnih podataka, no to se ne može sa sigurnošću utvrditi ili 2) kada su osobni podaci potrebni kao dokaz⁷⁶⁰.

Kad god voditelj obrade odbije ispraviti ili izbrisati osobne podatke ili ograničiti obradu podataka, ispitanika se o tome mora obavijestiti pisanim putem. Države članice mogu to pravo na informacije ograničiti radi, među ostalim, zaštite javne sigurnosti ili prava i sloboda drugih, iz istih razloga kao i kada se ograničava pravo na pristup⁷⁶¹.

Ispitanik obično ima pravo na informacije o obradi svojih osobnih podataka te ima pravo na pristup, ispravak ili brisanje podataka ili pak ograničavanje njihove obrade, koje može ostvariti izravno putem voditelja obrade. Druga mogućnost, neizravno ostvarivanje prava ispitanika putem nadzornog tijela za zaštitu podataka, dopuštena je na temelju Direktive o zaštiti podataka za policiju i tijela kaznenog prava, a počinje važiti kada voditelj obrade ograniči prava ispitanika⁷⁶². Člankom 17. Direktive propisuje se da države članice donose mjere kojima se osigurava da se prava ispitanika mogu ostvariti i putem nadležnog nadzornog tijela. Zbog toga voditelj obrade podataka mora obavijestiti ispitanika o mogućnosti neizravnog pristupa.

Obveze voditelja i izvršitelja obrade

U kontekstu Direktive o zaštiti podataka za policiju i tijela kaznenog pravosuđa voditelji su obrade nadležna javna tijela ili druga tijela s odgovarajućim javnim ovlastima i javnim vlastima, koja utvrđuju svrhe i načine obrade osobnih podataka. Direktivom se utvrđuje nekoliko obveza voditelja obrade kako bi se osigurala visoka razina zaštite osobnih podataka koji se obrađuju u svrhe izvršavanja zakonodavstva.

Nadležna tijela moraju voditi zapise o postupcima obrade koje provode putem automatiziranih sustava obrade. Zapisi se moraju bilježiti barem za prikupljanje, izmjene, obavljanje uvida, otkrivanje, uključujući prijenose, kombiniranje i brisanje osobnih

⁷⁵⁹ *Ibid.*, članak 16. stavak 2.

⁷⁶⁰ *Ibid.*, članak 16. stavak 3.

⁷⁶¹ *Ibid.*, članak 16. stavak 4.

⁷⁶² *Ibid.*, članak 17.

podataka⁷⁶³. Direktivom se također utvrđuje da zapisi o obavljanju uvida i otkrivanju moraju omogućiti da se ustanovi datum i vrijeme takvih postupaka, njihovo obrazloženje te, ako je to moguće, identitet osobe koja je obavila uvid ili otkrila osobne podatke i identitet primatelja takvih osobnih podataka. Zapisi se moraju upotrebljavati samo u svrhe provjere zakonitosti obrade, samopraćenja i osiguravanja cjelovitosti i sigurnosti osobnih podataka te za kaznene postupke⁷⁶⁴. Voditelj i izvršitelj obrade moraju na zahtjev staviti zapise na raspolaganje nadzornom tijelu.

Posebno je propisana opća obveza da voditelji obrade provedu odgovarajuće tehničke i organizacijske mjere kako bi osigurali da se obrada provodi u skladu s Direktivom te kako bi mogli dokazati zakonitost takve obrade⁷⁶⁵. Prilikom uspostavljanja takvih mjera, oni moraju uzeti u obzir prirodu, opseg i kontekst obrade te posebno moguće rizike za prava i slobode pojedinaca. Voditelji obrade trebaju donijeti interna pravila i provesti mjere koje olakšavaju sukladnost s načelima zaštite podataka, a posebice načelom tehničke i integrirane zaštite podataka⁷⁶⁶. Ako je vjerojatno da će obrada prouzročiti visok rizik za prava pojedinaca, primjerice zbog primjene novih tehnologija, voditelji obrade moraju provesti procjenu učinka zaštite podataka prije obrade⁷⁶⁷. U Direktivi se također navode mjere koje voditelji obrade moraju provesti kako bi osigurali sigurnost obrade. One uključuju mjere sprečavanja neovlaštenog pristupa osobnim podacima koje oni obrađuju, osiguravanja da ovlaštene osobe imaju pristup samo osobnim podacima koji su obuhvaćeni njihovim ovlaštenjem za pristup, da funkcije sustava obrade ispravno rade te da se pohranjeni osobni podaci ne mogu ugroziti zbog nedostataka u funkcioniranju sustava⁷⁶⁸. Ako ipak dođe do povrede osobnih podataka, voditelji obrade moraju obavijestiti nadzorno tijelo u roku od tri dana, navodeći prirodu povrede, njezine vjerojatne posljedice, kategorije zahvaćenih osobnih podataka i približan broj dotičnih ispitanika. O povredi osobnih podataka mora se obavijestiti i ispitanika, „bez nepotrebnog odgađanja“, ako je vjerojatno da će povreda prouzročiti visok rizik za njegova prava i slobode⁷⁶⁹.

Direktiva sadržava načelo odgovornosti, prema kojem voditelji obrade imaju dužnost provesti mjere kojima će osigurati sukladnost s tim načelom. Voditelji obrade moraju

⁷⁶³ *Ibid.*, članak 25. stavak 1.

⁷⁶⁴ *Ibid.*, članak 25. stavak 2.

⁷⁶⁵ *Ibid.*, članak 19.

⁷⁶⁶ *Ibid.*, članak 20.

⁷⁶⁷ *Ibid.*, članak 27.

⁷⁶⁸ *Ibid.*, članak 29.

⁷⁶⁹ *Ibid.*, članci 30. i 31.

voditi evidenciju o svim kategorijama aktivnosti obrade za koje su nadležni: detaljan sadržaj te evidencije utvrđen je u članku 24. Direktive. Evidencija se mora na zahtjev staviti na raspolaganje nadzornom tijelu kako bi ono moglo nadzirati postupke obrade voditelja obrade. Druga je važna mjera za povećanje odgovornosti imenovanje službenika za zaštitu podataka (SZP). Voditelji obrade moraju imenovati službenika za zaštitu podataka, iako se Direktivom omogućuje da države članice izuzmu sudove i druga neovisna pravosudna tijela od te obveze⁷⁷⁰. Dužnosti SZP-a slične su onima koje su utvrđene Općom uredbom o zaštiti podataka. Službenik nadzire usklađenost s Direktivom, pruža informacije i savjetuje zaposlenike koji provode obradu podataka o njihovim obvezama prema zakonodavstvu o zaštiti podataka. SZP također daje savjete o potrebi provedbe procjene učinka zaštite podataka i djeluje kao kontaktna točka nadzornog tijela.

Prijenosi trećim zemljama ili međunarodnim organizacijama

Slično kao i Općom uredbom o zaštiti podataka, Direktivom se utvrđuju uvjeti prijenosa osobnih podataka u treće zemlje ili međunarodne organizacije. Kad bi se osobni podaci slobodno prenosili izvan nadležnosti EU-a, mogle bi se narušiti zaštitne mjere i snažna zaštita osigurani pravom EU-a. Međutim, sami uvjeti znatno se razlikuju od onih iz Opće uredbе o zaštiti podataka. Prijenos osobnih podataka u treće zemlje ili međunarodne organizacije dopušten je⁷⁷¹:

- ako je prijenos nužan za ciljeve Direktive,
- ako se osobni podaci prenose nadležnom tijelu treće zemlje ili međunarodne organizacije u smislu Direktive, iako su moguća odstupanja od tog pravila u pojedinačnim i posebnim slučajevima⁷⁷²,
- ako je za prijenos osobnih podataka primljenih u okviru prekogranične suradnje trećim zemljama ili međunarodnim organizacijama potrebno odobrenje države članice iz koje podaci potječu, no postoje izuzeci u hitnim slučajevima,
- ako je Europska komisija donijela odluku o primjerenosti, ako su uspostavljene odgovarajuće zaštitne mjere ili se primjenjuje odstupanje za prijenose u posebnim situacijama,

⁷⁷⁰ *Ibid.*, članak 32.

⁷⁷¹ *Ibid.*, članak 35.

⁷⁷² *Ibid.*, članak 39.

- ako je za daljnje prijenose osobnih podataka trećoj zemlji ili međunarodnoj organizaciji potrebno prethodno odobrenje nadležnog tijela koje je izvršilo prvotni prijenos za koje će se, među ostalim, u obzir uzeti ozbiljnost kaznenog djela i razina zaštite podataka u odredišnoj zemlji drugog međunarodnog prijenosa podataka⁷⁷³.

Sukladno Direktivi, prijenosi osobnih podataka mogu se odvijati ako je ispunjen jedan od triju uvjeta. Prvi se odnosi na slučaj u kojemu je Europska komisija donijela odluku o primjerenosti na temelju Direktive. Odluka se može primjenjivati na cijelo državno područje ili određene sektore treće zemlje ili međunarodne organizacije. Međutim, to je moguće samo ako se osigura odgovarajuća razina zaštite i ako su ispunjeni uvjeti iz Direktive⁷⁷⁴. U takvim slučajevima prijenosi osobnih podataka ne podliježu odobrenju države članice⁷⁷⁵. Europska komisija mora pratiti razvoj događaja koji bi mogli utjecati na učinkovitost odluka o primjerenosti. Osim toga, odluka mora sadržavati mehanizam za periodično preispitivanje. Komisija također može staviti izvan snage, izmijeniti ili suspendirati odluku ako dostupne informacije upućuju na to da uvjeti u trećoj zemlji ili međunarodnoj organizaciji više ne osiguravaju odgovarajuću razinu zaštite. U tom slučaju Komisija mora započeti savjetovanje s trećom zemljom ili međunarodnom organizacijom radi popravljanja stanja.

Ako ne postoji odluka o primjerenosti, prijenosi se mogu temeljiti na odgovarajućim zaštitnim mjerama. One mogu biti utvrđene pravno obvezujućim instrumentom ili voditelj obrade može provesti samoprocjenu okolnosti prijenosa osobnih podataka i zaključiti da postoje odgovarajuće zaštitne mjere. Prilikom samoprocjene trebali bi se uzeti u obzir mogući sporazumi o suradnji sklopljeni između Europolu ili Eurojusta i treće zemlje ili međunarodne organizacije, postojanje obveza povjerljivosti i ograničenja svrhe te jamstva da se podaci neće upotrebljavati ni za koji oblik okrutnog i nečovječnog postupanja, uključujući izvršenje smrtno kazne⁷⁷⁶. U potonjem slučaju voditelj obrade mora obavijestiti nadležno nadzorno tijelo o kategorijama prijenosa na temelju ove kategorije⁷⁷⁷.

Čak i ako nije donesena odluka o primjerenosti ili nisu uspostavljene odgovarajuće zaštitne mjere, prijenosi se i dalje mogu dozvoliti u posebnim situacijama

773 *Ibid.*, članak 35. stavak 1.

774 *Ibid.*, članak 36.

775 *Ibid.*, članak 36. stavak 1.

776 *Ibid.*, uvodna izjava 71.

777 *Ibid.*, članak 37. stavak 1.

navedenima u Direktivi. One među ostalim uključuju zaštitu vitalnih interesa ispitanika ili druge osobe te sprečavanje neposredne i ozbiljne prijetnje javnoj sigurnosti države članice ili treće zemlje⁷⁷⁸.

U pojedinim i posebnim slučajevima prijenosi nadležnih tijela primateljima s nastanom u trećim zemljama koji nisu nadležna tijela mogu se vršiti ako su uz jedan od triju uvjeta koji su opisani iznad ispunjeni i dodatni uvjeti utvrđeni u članku 39. Direktive. Točnije, prijenos mora biti strogo nužan za obavljanje zadatka nadležnog tijela koje vrši prijenos, koje je također odgovorno za potvrdu da nikakva temeljna prava ili slobode pojedinaca nemaju prednost pred javnim interesom kojim se opravdava prijenos. Takvi se prijenosi moraju dokumentirati, a nadležno tijelo koje vrši prijenos mora obavijestiti nadležno nadzorno tijelo⁷⁷⁹.

Kad je riječ o trećim zemljama i međunarodnim organizacijama, Direktivom se također nalaže razvoj mehanizama međunarodne suradnje za olakšavanje djelotvornog izvršavanja zakonodavstva i pomaganje nadzornim tijelima za zaštitu podataka da surađuju sa sličnim tijelima u drugim zemljama⁷⁸⁰.

Neovisni nadzor i pravni lijekovi za ispitanike

Svaka država članica mora osigurati da je jedno ili više neovisnih nacionalnih nadzornih tijela odgovorno za savjetovanje i nadzor primjene odredbi usvojenih u skladu s Direktivom⁷⁸¹. Nadzorno tijelo uspostavljeno za potrebe Direktive može biti isto kao nadzorno tijelo uspostavljeno na temelju Opće uredbe o zaštiti podataka, no države članice imaju slobodu imenovanja drugog tijela, pod uvjetom da ono ispunjava kriterije neovisnosti. Nadzorna tijela moraju također saslušati zahtjeve koje podnese bilo koja osoba u vezi sa zaštitom njezinih prava i sloboda u pogledu obrade osobnih podataka koju vrše nadležna tijela.

Ako je ostvarenje prava ispitanika odbijeno iz opravdanih razloga, ispitanik mora imati pravo na žalbu nadležnom nacionalnom nadzornom tijelu i/ili sudu. Ako osoba pretrpi štetu zbog kršenja nacionalnog zakonodavstva kojim se provodi Direktiva, ima pravo na naknadu od voditelja obrade ili bilo kojeg drugog tijela nadležnog na

⁷⁷⁸ *Ibid.*, članak 38. stavak 1.

⁷⁷⁹ *Ibid.*, članak 37. stavak 3.

⁷⁸⁰ *Ibid.*, članak 40.

⁷⁸¹ *Ibid.*, članak 41.

temelju zakonodavstva države članice⁷⁸². Općenito, ispitanici moraju imati na raspolaganju pravni lijek u slučaju bilo kojeg kršenja prava koja su im zajamčena nacionalnim zakonodavstvom kojim se provodi Direktiva⁷⁸³.

8.3. Ostali specifični pravni instrumenti za zaštitu podataka u slučajevima izvršavanja zakonodavstva

Osim Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa, razmjena informacija koje države članice posjeduju u posebnim područjima uređena je nizom pravnih instrumenata, kao što su: Okvirna odluka Vijeća 2009/315/PUP o organizaciji i sadržaju razmjene podataka iz kaznene evidencije između država članica, Odluka Vijeća 2000/642/PUP o uređenju suradnje između financijsko-obavještajnih jedinica država članica vezano za razmjenu informacija te Okvirna odluka Vijeća 2006/960/PUP od 18. prosinca 2006. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije⁷⁸⁴.

Važno je napomenuti da prekogranična suradnja⁷⁸⁵ nadležnih tijela sve više uključuje razmjenu imigracijskih podataka. To područje prava ne smatra se nadležnošću policijskih i kaznenopravnih predmeta, no u mnogočemu je relevantno za rad policije i pravosudnih tijela. Isto vrijedi za podatke o robi koja se uvozi u Europsku uniju ili izvozi iz nje. Ukidanjem unutarnjih graničnih kontrola u schengenskom prostoru povećan je rizik od prijevare pa države članice moraju pojačati suradnju, naročito poboljšanjem prekogranične razmjene podataka radi učinkovitijeg otkrivanja i progona kršenja nacionalnog carinskog prava i carinskog prava Europske unije. Usto, u proteklih nekoliko godina vidljiv je porast teškog i organiziranog kriminala

782 *Ibid.*, članak 56.

783 *Ibid.*, članak 54.

784 Vijeće Europske unije (2009.), Okvirna odluka Vijeća 2009/315/PUP od 26. veljače 2009. o organizaciji i sadržaju razmjene podataka iz kaznene evidencije između država članica, SL 2009 L 93; Vijeće Europske unije (2000.), Odluka Vijeća 2000/642/PUP od 17. listopada 2000. o uređenju suradnje između financijsko-obavještajnih jedinica država članica vezano za razmjenu informacija, SL 2000 L 271; Okvirna odluka Vijeća 2006/960/PUP od 18. prosinca 2006. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije, SL L 386.

785 Europska komisija (2012.), *Komunikacija Komisije Europskom parlamentu i Vijeću, „Jačanje pravosudne suradnje u Europskoj uniji: Europski model za razmjenu informacija (EIXM)”, COM(2012) 735 final, Bruxelles, 7. prosinca 2012.*

i terorizma, koji mogu uključivati međunarodna putovanja, te je u mnogim slučajevima uočena potreba za povećanom prekograničnom suradnjom policije i tijela za izvršavanje zakonodavstva⁷⁸⁶.

Prümska odluka

Važan primjer institucionalizacije prekogranične suradnje razmjenom podataka koji se čuvaju na nacionalnoj razini jest Odluka Vijeća 2008/615/PUP, zajedno s odredbama za provođenje iz Odluke 2008/616/PUP, o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma i prekograničnog kriminala (Prümska odluka), kojom je Prümski ugovor ugrađen u pravo EU-a 2008.⁷⁸⁷ Prümski ugovor jest ugovor o međunarodnoj policijskoj suradnji koji su 2005. potpisali Austrija, Belgija, Francuska, Njemačka, Luksemburg, Nizozemska i Španjolska⁷⁸⁸.

Cilj je Prümske odluke pomoći državama potpisnicama u poboljšanju razmjene informacija radi sprečavanja i suzbijanja kriminala u trima područjima: terorizmu, prekograničnom kriminalu i nezakonitoj migraciji. U tu se svrhu u odluci navode odredbe u pogledu:

- automatiziranog pristupa DNK profilima, podacima o otiscima prstiju i određenim nacionalnim podacima o registraciji vozila,
- dostave podataka u vezi s važnim događajima prekogranične naravi,
- dostave informacija radi sprečavanja terorističkih kaznenih djela,
- drugih mjera za produbljivanje prekogranične policijske suradnje.

Za baze podataka koje se stavljaju na raspolaganje prema Prümskoj odluci u potpunosti je nadležno nacionalno zakonodavstvo, no razmjena podataka dodatno je uređena odlukom, čija će se sukladnost s Direktivom o zaštiti podataka za policiju

786 Vidjeti Europska komisija (2011.), Prijedlog direktive Europskog parlamenta i Vijeća o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela, COM(2011) 32 final, Bruxelles, 2. veljače 2011., str. 1.

787 Vijeće Europske unije (2008.), Odluka Vijeća 2008/615/PUP od 23. lipnja 2008. o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma i prekograničnog kriminala, SL 2008 L 210.

788 Konvencija (dostupna na engleskom jeziku) između Kraljevine Belgije, Savezne Republike Njemačke, Kraljevine Španjolske, Francuske Republike, Velikog Vojvodstva Luksemburga, Kraljevine Nizozemske i Republike Austrije o produbljivanju prekogranične suradnje, posebno u suzbijanju terorizma, prekograničnog kriminala i nezakonite migracije.

i tijela kaznenog pravosuđa morati procijeniti. Tijela nadležna za nadzor takvih prijenosa podataka nacionalna su nadzorna tijela za zaštitu podataka.

Okvirna odluka 2006/960/PUP – Švedska inicijativa

Okvirna odluka 2006/960/PUP (Švedska inicijativa)⁷⁸⁹ predstavlja još jedan primjer prekogranične suradnje u pogledu razmjene podataka koje tijela za izvršavanje zakonodavstva posjeduju na nacionalnoj razini. Švedska inicijativa posebno je usmjerena na razmjenu obavještajnih podataka i informacija te se njezinim članom 8. propisuju posebni propisi o zaštiti podataka.

Sukladno tom instrumentu, upotreba razmijenjenih informacija i obavještajnih podataka mora podlijeagati nacionalnim odredbama za zaštitu podataka u državi članici koja prima informacije, u skladu s istim propisima koji bi vrijedili i da su podaci prikupljeni u toj državi članici. U članku 8. dalje se navodi da prilikom dostavljanja informacija i obavještajnih podataka nadležno tijelo za izvršavanje zakonodavstva može, sukladno svojem nacionalnom zakonodavstvu, odrediti uvjete za njihovu upotrebu nadležnom tijelu za izvršavanje zakonodavstva koje ih prima. Ti se uvjeti mogu primjenjivati i na izvješćivanje o rezultatima istrage o kaznenom djelu ili operacijama prikupljanja obavještajnih podataka o kaznenom djelu za koje je bila potrebna razmjena informacija i obavještajnih podataka. Međutim, u slučajevima u kojima se nacionalnim zakonodavstvom propisuju izuzeća za ograničenje upotrebe (npr. za pravosudna tijela, zakonodavna tijela itd.), informacije i obavještajni podaci mogu se upotrebljavati samo nakon prethodnog savjetovanja s državom članicom koja ih dostavlja.

Dostavljene informacije i obavještajni podaci mogu se upotrebljavati:

- za svrhe za koje su dostavljeni, ili
- za sprečavanje neposredne i ozbiljne opasnosti za javnu sigurnost.

Obrada u druge svrhe može se dopustiti samo uz prethodno odobrenje države članice koja ih dostavlja.

⁷⁸⁹ Vijeće Europske unije (2006.), Okvirna odluka Vijeća 2006/960/PUP od 18. prosinca 2006. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije, SL L 386/89 od 29. prosinca 2006.

U Švedskoj inicijativi dalje se navodi da se obrađeni osobni podaci moraju zaštititi u skladu s međunarodnim instrumentima kao što su:

- Konvencija Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka⁷⁹⁰,
- Dodatni protokol uz tu Konvenciju od 8. studenoga 2001. koji se tiče nadzornih tijela i prekograničnih prijenosa podataka⁷⁹¹,
- Preporuka br. R(87) 15 Vijeća Europe o korištenju osobnih podataka u sektoru policije⁷⁹².

Direktiva Europske unije o evidenciji podataka o putnicima

Podaci iz evidencije podataka o putnicima (PNR) odnose se na informacije o putnicima u zračnom prometu koji se prikupljaju i čuvaju u sustavima rezervacija i kontrole odlazaka zračnih prijevoznika u njihove vlastite komercijalne svrhe. Oni sadrže nekoliko različitih vrsta podataka, kao što su datumi putovanja, plan putovanja, informacije o kartama, podaci za kontakt, informacije o putničkoj agenciji putem koje je let rezerviran, informacije o načinu plaćanja, broj sjedala i informacije o prtljazi⁷⁹³. Obrada podataka iz evidencije podataka o putnicima može pomoći tijelima za izvršavanje zakonodavstva da identificiraju poznate ili potencijalne osumnjičene i provedu procjene na temelju obrazaca putovanja i drugih pokazatelja koji se obično povezuju s kriminalnim aktivnostima. Analiza podataka iz evidencije također omogućuje retrospektivno praćenje pravaca putovanja i kontakata osoba koje su osumnjičene za sudjelovanje u kriminalnim aktivnostima, što tijelima za izvršavanje zakonodavstva može pomoći u otkrivanju kriminalnih mreža⁷⁹⁴. EU je sklopio određene sporazume s trećim zemljama u svrhu razmjene podataka iz evidencije podataka

790 Vijeće Europe (1981.), Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, ETS br. 108.

791 Vijeće Europe (2001.), Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, ETS br. 108.

792 Vijeće Europe (1987.), Preporuka br. R(87) 15 Odbora ministara o korištenju osobnih podataka u sektoru policije (koju je donio Odbor ministara 17. rujna 1987. na 410. sastanku zamjenika ministara).

793 Europska komisija (2011.), Prijedlog direktive Europskog parlamenta i Vijeća o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela, COM(2011) 32 final, Bruxelles, 2. veljače 2011., str. 1.

794 Europska komisija (2015.), *Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives* (Informativni list „Borba protiv terorizma na razini EU-a: pregled djelovanja, mjera i inicijativa Komisije”), Bruxelles, 11. siječnja 2015.

o putnicima, kako je objašnjeno u [dijelu 7](#). Osim toga, Unija je uvela i obradu podataka iz PNR-a na području EU-a u sklopu Direktive 2016/681/EU o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela (Direktiva EU-a o evidenciji podataka o putnicima)⁷⁹⁵. Tom se Direktivom zračnim prijevoznicima propisuju obveze prijenosa podataka iz PNR-a nadležnim tijelima i uspostavljaju stroge mjere za zaštitu podataka za potrebe obrade i prikupljanja takvih podataka. Direktiva EU-a o evidenciji podataka o putnicima primjenjuje se na međunarodne letove u EU i iz EU-a, kao i na letove unutar Unije ako država članica tako odluči⁷⁹⁶.

Prikupljeni podaci iz PNR-a smiju sadržavati samo informacije dopuštene Direktivom EU-a o evidenciji podataka o putnicima. Moraju se čuvati u jedinstvenom odjelu za informacije na sigurnoj lokaciji u svakoj državi članici. Podaci iz PNR-a moraju se depersonalizirati šest mjeseci nakon što ih zračni prijevoznik prenese i čuvati najviše pet godina⁷⁹⁷. Podaci iz PNR-a razmjenjuju se među državama članicama, između država članica i Europolu te s trećim zemljama, no samo na osnovi pojedinih slučajeva.

Prijenos i obrada podataka iz PNR-a te prava zaštićena za ispitanike moraju biti u skladu s Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa te se njima mora osigurati visoka razina zaštite privatnosti osobnih podataka koja se propisuje Poveljom, Moderniziranom Konvencijom br. 108 i EKLJP-om.

Neovisna nacionalna nadzorna tijela koja su nadležna na temelju Direktive o zaštiti podataka za policiju i tijela kaznenog pravosuđa također su odgovorna za savjetovanje o odredbama koje donesu države članice i praćenje njihove primjene, sukladno Direktivi EU-a o evidenciji podataka o putnicima.

⁷⁹⁵ Direktiva (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela, SL L 119, str. 132.

⁷⁹⁶ Direktiva o evidenciji podataka o putnicima, L 119, str. 132, članak 1. stavak 1. i članak 2. stavak 1.

⁷⁹⁷ *Ibid.*, članak 12. stavak 1. i članak 12. stavak 2.

Zadržavanje telekomunikacijskih podataka

Prema Direktivi o zadržavanju podataka⁷⁹⁸, koja je proglašena nevaljanom 8. travnja 2014. u okviru predmeta *Digital Rights Ireland*, pružatelji komunikacijskih usluga bili su dužni staviti na raspolaganje metapodatke u posebnu svrhu suzbijanja teškog kriminala, tijekom razdoblja od najmanje šest mjeseci i najviše 24 mjeseca, bez obzira na to jesu li pružatelju ti podaci i dalje bili potrebni u svrhu naplate ili tehničkog pružanja usluge.

Zadržavanje telekomunikacijskih podataka predstavlja jasno miješanje u pravo na zaštitu podataka⁷⁹⁹. Je li takvo miješanje opravdano osporavalo se u nekoliko sudskih postupaka u državama članicama⁸⁰⁰.

Primjer: U predmetu *Digital Rights Ireland i Kärntner Landesregierung i drugi*⁸⁰¹, grupa Digital Rights i g. Seitlinger pokrenuli su sudski postupak pred Visokim sudom u Irskoj odnosno pred Ustavnim sudom u Austriji, osporavajući zakonitost nacionalnih mjera kojima se omogućuje zadržavanje elektroničkih telekomunikacijskih podataka. Grupa Digital Rights zatražila je od irskoga suda da proglasi nevaljanom Direktivu 2006/24/EZ i dio nacionalnog kaznenog prava u vezi s terorističkim kaznenim djelima. Na sličan su način g. Seitlinger i više od 11 000 drugih tužitelja osporili i zatražili poništavanje odredbe austrijskog zakonodavstva o telekomunikacijama kojim je prenesena Direktiva 2006/24/EZ.

Prilikom rješavanja tih zahtjeva za prethodne odluke, SEU je proglasio Direktivu o zadržavanju podataka nevaljanom. Prema SEU-u, podaci koji su se mogli zadržavati na temelju Direktive pružali su točne informacije o pojedincima kada su se razmatrali kao cjelina. SEU je nadalje razmatrao ozbiljnost miješanja u temeljna prava na poštovanje privatnog života i zaštitu osobnih

798 Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ, SL 2006 L 105.

799 EDPS (2011.), Mišljenje od 31. svibnja 2011. o Evaluacijskom izvješću Komisije Vijeću i Europskom parlamentu o Direktivi o zadržavanju podataka (Direktiva 2006/24/EZ), 31. svibnja 2011.

800 Njemačka, Savezni ustavni sud (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. ožujka 2010.; Rumunjska, Savezni ustavni sud (*Curtea Constituțională a României*), br. 1258, 8. listopada 2009.; Češka Republika, Ustavni sud (*Ústavní soud České republiky*), 94/2011 Coll., 22. ožujka 2011.

801 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [V], 8. travnja 2014., t. 65.

podataka. Zaključio je da se zadržavanjem podataka ostvaruje cilj javnog interesa, odnosno borbe protiv teškog kriminala, a time i javne sigurnosti. Unatoč tome, SEU je utvrdio da je zakonodavac EU-a donošenjem Direktive prekršio načelo proporcionalnosti. Iako je Direktiva mogla biti primjereno sredstvo za ostvarenje željenog cilja, „opsežno i posebno ozbiljno miješanje Direktive u temeljna prava na poštovanje privatnosti i zaštitu osobnih podataka nije dovoljno ograničeno kako bi se osiguralo da je miješanje doista ograničeno na ono što je strogo nužno“.

Zadržavanje podataka dopušteno je, u nedostatku posebnog zakonodavstva o zadržavanju podataka, kao izuzeće od povjerljivosti telekomunikacijskih podataka na temelju Direktive 2002/58/EZ (Direktiva o privatnosti i elektroničkim komunikacijama)⁸⁰², kao preventivna mjera, no mora se vršiti isključivo u svrhu borbe protiv teških kaznenih djela. Takvo zadržavanje podataka mora biti ograničeno na ono što je strogo nužno s obzirom na kategorije zadržanih podataka, obuhvaćeno sredstvo komunikacije, dotične osobe i odabrano razdoblje zadržavanja. Nacionalna tijela mogu imati pristup zadržanim podacima u strogo kontroliranim uvjetima, uključujući prethodni pregled neovisnog tijela. Podaci se moraju čuvati unutar EU-a.

Primjer: Nakon presude u predmetu *Digital Rights Ireland* i *Kärntner Landesregierung i drugi*⁸⁰³ pred SEU-om su pokrenuta dodatna dva predmeta u vezi s općom obvezom koja je u Švedskoj i Ujedinjenoj Kraljevini nametnuta pružateljima elektroničkih komunikacijskih usluga za zadržavanje telekomunikacijskih podataka, kako je bilo propisano Direktivom o zadržavanju podataka koja je proglašena nevaljanom. U predmetima *Tele2 Sverige* i *Home Department protiv Toma Watsona i drugih*⁸⁰⁴ SEU je presudio da nacionalno zakonodavstvo kojim se propisuje opće i neselektivno zadržavanje podataka bez uvjetovanja bilo kakva odnosa između podataka koji se moraju zadržati i prijetnje javnoj sigurnosti, kao i bez utvrđivanja bilo kakvih uvjeta – npr. razdoblja zadržavanja, zemljopisnog područja, skupine osoba za koje je vjerojatno da će biti uključene u teška kaznena djela – premašuje granice strogo

802 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL 2002 L 201.

803 SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources* i dr. i *Kärntner Landesregierung* i dr. [VV], 8. travnja 2014.

804 SEU, spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen* i *Secretary of State for the Home Department protiv Toma Watsona* i dr. [VV], 21. prosinca 2016.

nužnog i ne može se smatrati opravdanim u demokratskom društvu, kako se propisuje Direktivom 2002/58/EZ, kada se tumači u smislu Povelje EU-a o temeljnim pravima.

Izgledi

U siječnju 2017. Europska komisija objavila je Prijedlog uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama, kojom bi se stavila izvan snage i zamijenila Direktiva 2002/58/EZ⁸⁰⁵. Prijedlog ne sadržava nikakve posebne odredbe o zadržavanju podataka. Međutim, u njemu se utvrđuje da države članice mogu zakonom ograničiti određene obveze i prava na temelju Uredbe ako takvo ograničenje čini nužnu i proporcionalnu mjeru za zaštitu posebnih javnih interesa, uključujući nacionalnu sigurnost, obranu, javnu sigurnost te sprečavanje, istragu, otkrivanje i progon kaznenih djela ili izvršavanja kaznenopravnih sankcija⁸⁰⁶. Tako bi države članice mogle zadržati ili stvoriti nacionalne okvire za zadržavanje podataka kojima se utvrđuju ciljne mjere zadržavanja, u mjeri u kojoj bi takvi okviri bili u skladu s pravom Unije, uzimajući u obzir sudsku praksu SEU-a u vezi s tumačenjem Direktive o privatnosti i elektroničkim komunikacijama i Povelju EU-a o temeljnim pravima⁸⁰⁷. U vrijeme izrade ovog priručnika rasprave o donošenju Uredbe još su bile u tijeku.

Krovni sporazum između SAD-a i EU-a o zaštiti osobnih informacija u svrhe kaznenog progona

Krovni sporazum između SAD-a i Europske unije o obradi osobnih podataka u svrhu sprečavanja, istrage, otkrivanja i progona kaznenih djela stupio je na snagu 1. veljače 2017.⁸⁰⁸ Krovnim sporazumom između SAD-a i EU-a nastoji se osigurati visoka razina zaštite podataka za građane EU-a i istovremeno poboljšati suradnja nacionalnih tijela za izvršavanje zakonodavstva EU-a i SAD-a. Njime se dopunjuju

805 Europska komisija (2017.), Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), COM(2017) 10 final, Bruxelles, 10. siječnja 2017.

806 *Ibid.*, uvodna izjava 26.

807 Vidjeti Memorandum s objašnjenjima o Prijedlogu uredbe o privatnosti i elektroničkim komunikacijama COM(2017) 10 final, točka 1.3.

808 Vidjeti Vijeće EU-a (2016.), *Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'* (Poboljšana prava zaštite podataka za građane EU-a temeljem suradnje tijela za izvršavanje zakonodavstva: potpisivanje „Krovnog sporazuma” između EU-a i SAD-a), priopćenje za medije 305/16, 2. lipnja 2016.

postojeći sporazumi između EU-a i SAD-a te država članica i SAD-a sklopljeni među tijelima za izvršavanje zakonodavstva te se istovremeno uspostavljaju jasni i usklađeni propisi za zaštitu podataka za buduće sporazume u tom području. Kad je riječ o tome, sporazumom se nastoji utvrditi trajan pravni okvir za olakšanu razmjenu informacija.

Sam sporazum ne pruža prikladnu pravnu osnovu za razmjenu osobnih podataka, no pruža odgovarajuće mjere za zaštitu podataka pojedincima na koje se to odnosi. On obuhvaća svu obradu osobnih podataka nužnu za sprečavanje, istragu, otkrivanje i progon kaznenih djela, uključujući terorizam⁸⁰⁹.

Sporazumom se utvrđuje nekoliko zaštitnih mjera kako bi se osiguralo da se osobni podaci upotrebljavaju isključivo u svrhe utvrđene u Sporazumu. Njime se građanima EU-a pružaju posebno sljedeće zaštite:

- ograničenja upotrebe podataka: osobni podaci mogu se upotrebljavati samo u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela,
- zaštita od proizvoljne i neopravdane diskriminacije,
- daljnji prijenosi: za svaki daljnji prijenos u zemlju izvan SAD-a i EU-a ili međunarodnu organizaciju mora se ishoditi prethodna privola nadležnog tijela zemlje koja je izvorno prenijela podatke,
- kvaliteta podataka: osobni podaci moraju se čuvati tako da se u obzir uzmu njihova točnost, relevantnost, ažurnost i cjelovitost,
- sigurnost obrade, uključujući obavijest o povredama osobnih podataka,
- obrada osjetljivih podataka dopuštena je samo uz odgovarajuće zaštitne mjere u skladu sa zakonom,

809 Sporazum između Sjedinjenih Američkih Država i Europske unije o zaštiti osobnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i progonom kaznenih djela od 18. svibnja 2016., (OR.en) 8557/16, članak 3. stavak 1. Vidjeti i Obavijest Komisije o pregovorima o sporazumu za zaštitu podataka između EU-a i SAD-a od 26. svibnja 2010., MEMO/10/216 i Priopćenje za medije Europske komisije (2010.) o visokim standardima privatnosti u sporazumu o zaštiti podataka između EU-a i SAD-a od 26. svibnja 2010., IP/10/609.

- razdoblja zadržavanja: osobni podaci ne smiju se zadržavati dulje nego što je nužno ili primjereno,
- prava na pristup i ispravak: svaki pojedinac ima pravo na pristup svojim osobnim podacima pod određenim uvjetima te će moći zatražiti ispravljanje podataka ako su netočni,
- za automatizirane odluke potrebne su odgovarajuće zaštitne mjere, uključujući mogućnost ljudske intervencije,
- učinkovit nadzor, uključujući suradnju između nadzornih tijela EU-a i SAD-a, te
- sudska zaštita i provedivost: građani EU-a imaju pravo⁸¹⁰ zatražiti sudsku zaštitu pred sudovima u SAD-u u slučajevima u kojima nadležna tijela SAD-a uskrate pristup ili ispravak ili nezakonito otkriju njihove osobne podatke.

Prema „Krovnom sporazumu” uspostavljen je i sustav za obavještanje nadležnog nadzornog tijela države članice u kojoj se nalaze dotični pojedinci o svim povredama zaštite podataka, kada je to potrebno. Pravnim zaštitnim mjerama koje su utvrđene Sporazumom osigurava se jednako postupanje prema građanima EU-a u SAD-u u slučaju povrede privatnosti⁸¹¹.

8.3.1. Zaštita podataka u pravosudnim tijelima i agencijama za izvršavanje zakonodavstva EU-a Europol

Europol, tijelo za izvršavanje zakonodavstva Europske unije sa sjedištem u Haagu ima Europolove nacionalne jedinice (ENU-e) u svakoj državi članici. Europol je osnovan 1998. Njegov trenutni pravni status institucije Europske unije temelji se na Uredbi o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva

810 Zakon SAD-a o sudskoj zaštiti ([US Judicial Redress Act](#)) stupio je na snagu potpisom predsjednika Obame 24. veljače 2016.

811 Europski nadzornik za zaštitu podataka izdao je Mišljenje o Sporazumu između EU-a i SAD-a kojim je, među ostalim, preporučio sljedeće izmjene: 1) dodavanje teksta „u posebne svrhe u koje su preneseni” u članak koji se odnosi na zadržavanje podataka ne dulje nego što je nužno i primjereno; 2) izuzimanje skupnog prijenosa osjetljivih podataka, što je možda moguće. Vidjeti: Europski nadzornik za zaštitu podataka, [Mišljenje 1/2016](#) (dostupno na engleskom jeziku), Preliminarno mišljenje o Sporazumu između Sjedinjenih Američkih Država i Europske unije o zaštiti osobnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i progonom kaznenih djela, članak 35.

(Uredba o Europolu)⁸¹². Cilj je Eurola pomoći u sprečavanju i istrazi organiziranog kriminala, terorizma i drugih oblika teških kaznenih djela koja utječu na dvije ili više država članica, a koja su navedena u Prilogu I. Uredbi o Europolu. To se postiže razmjenom informacija i njegovom ulogom informacijske središnjice EU-a koja pruža analize obavještajnih podataka i procjene prijetnji.

Radi ostvarenja svojih ciljeva Europol je uspostavio Europolov informacijski sustav s bazom podataka na temelju koje države članice razmjenjuju kriminalističke obavještajne podatke i informacije putem svojih ENU-a. Europolov informacijski sustav može se upotrebljavati radi stavljanja na raspolaganje podataka koji se odnose na: osobe koje su osumnjičene ili osuđene za kazneno djelo u nadležnosti Eurola ili osobe za koje se opravdano sumnja da će takva djela počiniti. Europol i ENU-i mogu izravno unositi podatke u Europolov sustav informacija i preuzimati ih iz njega. Podatke može izmijeniti, ispraviti ili izbrisati samo stranka koja ih je unijela u sustav. Tijela EU-a, treće zemlje i međunarodne organizacije također mogu pružati informacije Europolu.

Europol može prikupljati informacije i osobne podatke i iz javno dostupnih izvora poput interneta. Prijenosi osobnih podataka tijelima EU-a dopušteni su samo ako je to nužno za izvršavanje zadatka Eurola ili tijela EU-a koje podatke prima. Prijenosi osobnih podataka u treće zemlje ili međunarodne organizacije dopušteni su samo ako Europska komisija odluči da ta zemlja ili međunarodna organizacija osigurava odgovarajuću razinu zaštite podataka („odluka o primjerenosti“) ili ako postoji međunarodni sporazum ili sporazum o suradnji. Europol može primati i obrađivati osobne podatke privatnih stranki i fizičkih osoba pod strogo određenim uvjetima prema kojima te podatke mora prenositi ENU u skladu sa svojim nacionalnim zakonodavstvom, kontaktna točka u trećoj zemlji ili međunarodna organizacija s kojom je uspostavljena suradnja putem sporazuma o suradnji, ili tijelo treće zemlje ili međunarodna organizacija koja podliježe odluci o primjerenosti ili s kojom je EU sklopio međunarodni sporazum. Sve razmjene informacija vrše se putem mrežne aplikacije za sigurnu razmjenu informacija (*Secure Information Exchange Network Application*, SIENA).

812 Uredba (EU) 2016/794 Europskog parlamenta i Vijeća od 11. svibnja 2016. o Agenciji Europske unije za suradnju tijela za izvršavanje zakonodavstva (Europol) te zamjeni i stavljanju izvan snage odluka Vijeća 2009/371/PUP, 2009/934/PUP, 2009/935/PUP, 2009/936/PUP i 2009/968/PUP, SL 2016 L 135, str. 53.

Kao odgovor na nove pojave, unutar Europolu osnovani su specijalizirani centri. Europski centar za kibernetički kriminal osnovan je unutar Europolu 2013.⁸¹³ Centar ima ulogu središta Europske unije za kibernetički kriminal, čime se omogućuje brže reagiranje u slučaju internetskih zločina, razvijanje i primjena digitalnih forenzičkih rješenja i provodi najbolja praksa u istragama kibernetičkog kriminala. Centar se bavi kibernetičkim kriminalom koji:

- počinje organizirane skupine radi ostvarivanja velike kriminalnih dobiti, kao što je internetska prijevarena,
- uzrokuje veliku štetu žrtvi, poput seksualnog iskorištavanja djece putem interneta,
- utječe na ključnu infrastrukturu ili informacijske sustave u Europskoj uniji.

Europski centar za borbu protiv terorizma (ECTC) osnovan je u siječnju 2016. radi pružanja operativne potpore državama članicama u istragama povezanim s terorističkim kaznenim djelima. Centar provodi unakrsne provjere aktualnih operativnih podataka u odnosu na podatke koje Europol već posjeduje, čime se brzo otkrivaju tragovi financiranja, te analizira sve dostupne pojedinosti istrage kako bi pomogao o stvaranju strukturiranog pregleda terorističke mreže⁸¹⁴.

Europski centar za borbu protiv krijumčarenja migranata (EMSC) osnovan je u veljači 2016., nakon sastanka Vijeća u studenom 2015., kako bi se državama članicama pomoglo u otkrivanju i uništavanju zločinačkih mreža uključenih u krijumčarenje migranata. Centar djeluje kao informacijska središnjica koja pruža potporu uredima regionalnih jedinica EU-a u Cataniji (Italija) i Pireju (Grčka), koji pomažu nacionalnim tijelima u nekoliko područja, uključujući dijeljenje obavještajnih podataka, istrage kaznenih djela i progon zločinačkih mreža za krijumčarenje ljudi⁸¹⁵.

Sustav zaštite podataka kojim se uređuju aktivnosti Europolu proširen je i temelji se na načelima Uredbe o zaštiti podataka u institucijama EU-a⁸¹⁶, a u skladu je i s Direkti-

813 Vidjeti i EDPS (2012.), *Mišljenje Nadzornika za zaštitu podataka o priopćenju Europske komisije Vijeću i Europskom parlamentu o osnivanju Europskog centra za kibernetički kriminal*, Bruxelles, 29. lipnja 2012.

814 Vidjeti Europolovu internetsku stranicu za ECTC.

815 Vidjeti Europolovu internetsku stranicu za EMSC.

816 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

vom o zaštiti podataka za policiju i tijela kaznenog pravosuđa, Moderniziranom Konvencijom br. 108 i Preporukom o policiji.

Obrada osobnih podataka u pogledu žrtava kaznenih djela, svjedoka ili drugih osoba koje mogu pružiti informacije o kaznenim djelima ili u pogledu osoba mlađih od 18 godina dopuštena je ako je to izričito nužno i razmjerno radi sprečavanja ili suzbijanja kriminaliteta koji potpada pod ciljeve Europol⁸¹⁷. Obrada osjetljivih osobnih podataka zabranjena je osim ako je to izričito nužno i razmjerno radi sprečavanja ili suzbijanja vrsta kaznenih djela obuhvaćenih ciljevima Europol⁸¹⁸. U obama slučajevima samo Europol može pristupiti relevantnim podacima⁸¹⁹.

Pohrana podataka dopuštena je samo onoliko dugo koliko je potrebno i razmjerno, a daljnje se pohranjivanje preispituje svake tri godine. Bez tog preispitivanja podaci se automatski brišu⁸²⁰.

Europol u određenim uvjetima može izravno prenositi osobne podatke tijelu EU-a ili tijelu treće zemlje ili međunarodnoj organizaciji⁸²¹. Ako bi kršenje osobnih podataka vjerojatno znatno i negativno utjecalo na prava i slobode dotičnih ispitanika, o tome ih se mora obavijestiti bez nepotrebnog odlaganja⁸²². Na razini država članica imenovat će se nacionalno nadzorno tijelo koje će nadzirati Europolovu obradu osobnih podataka⁸²³.

EDPS je odgovoran za nadzor i osiguravanje zaštite temeljnih prava i sloboda fizičkih osoba u pogledu obrade osobnih podataka koju obavlja Europol, kao i za savjetovanje Europol⁸²⁴ i ispitanika o svim pitanjima koja se odnose na obradu osobnih podataka. U tu svrhu EDPS djeluje kao tijelo za istrage i pritužbe te blisko surađuje s nacionalnim nadzornim tijelima⁸²⁴. EDPS i nacionalna nadzorna tijela sastaju se najmanje dvaput godišnje u okviru Odbora za suradnju koji ima savjetodavnu

817 Uredba o Europolu, članak 30. stavak 1.

818 *Ibid.*, članak 30. stavak 2.

819 *Ibid.*, članak 30. stavak 3.

820 *Ibid.*, članak 31.

821 *Ibid.*, članak 24. odnosno članak 25.

822 *Ibid.*, članak 35.

823 *Ibid.*, članak 42.

824 *Ibid.*, članak 43. i članak 44.

funkciju⁸²⁵. Države članice dužne su zakonom uspostaviti nadzorno tijelo koje je nadležno za praćenje dopustivosti prijenosa osobnih podataka s razine države Euro-polu te prikupljanja osobnih podataka i priopćavanja Europolu osobnih podataka od strane dotične države članice⁸²⁶. Države članice također moraju osigurati da nacionalno nadzorno tijelo može djelovati posve neovisno u ispunjavanju svojih zadaća i dužnosti na temelju Uredbe o Europolu⁸²⁷. Kako bi provjerio zakonitost obrade podataka, samostalno pratio svoje aktivnosti i osigurao cjelovitost i sigurnost podataka, Europol vodi evidenciju ili dokumentaciju o svojim aktivnostima obrade podataka. Ta evidencija sadržava informacije o postupcima obrade u sustavima automatizirane obrade, a odnosi se na sakupljanje, izmjene, pristup, otkrivanje, kombinaciju i brisanje⁸²⁸.

Pred SEU-om se može iznijeti žalba na odluku EDPS-a⁸²⁹. Svaka osoba koja je pretrpjela štetu kao posljedicu nezakonitih radnji obrade podataka ima pravo na primanje nadoknade za pretrpljenu štetu, bilo od Eurola ili od odgovorne države članice, tako da pokrene postupak pred SEU-om (prvi slučaj) ili pred nadležnim nacionalnim sudom (drugi slučaj)⁸³⁰. Usto, specijalizirana Zajednička skupina za parlamentarni nadzor (JPSG) nacionalnih parlamenata i Europskog parlamenta može nadzirati aktivnosti Eurola⁸³¹. Svaka osoba ima pravo na pristup svim osobnim podacima koje Europol čuva o njoj te pravo zatražiti da se ti osobni podaci provjere, isprave ili izbrišu. Ta prava mogu podlijegati izuzećima i ograničenjima.

Eurojust

Eurojust je tijelo Europske unije osnovano 2002., sa sjedištem u Haagu. Ono promiče pravosudnu suradnju u istragama i progonima teških kaznenih djela koja uključuju barem dvije države članice⁸³². Eurojust je nadležan za sljedeće:

825 *Ibid.*, članak 45.

826 *Ibid.*, članak 42. stavak 1.

827 *Ibid.*, članak 42. stavak 1.

828 *Ibid.*, članak 40.

829 *Ibid.*, članak 48.

830 *Ibid.*, članak 50.

831 *Ibid.*, članak 51.

832 Vijeće Europske unije (2002.), Odluka Vijeća 2002/187/PUP od 28. veljače 2002. kojom se osniva Eurojust s ciljem jačanja borbe protiv teških kaznenih djela, SL 2002 L 63; Vijeće Europske unije (2003.), Odluka Vijeća 2003/659/PUP od 18. lipnja 2003. o izmjeni Odluke 2002/187/PUP kojom se osniva Eurojust s ciljem jačanja borbe protiv teških kaznenih djela, SL 2003 L 44; Vijeće Europske unije (2009.), Odluka Vijeća 2009/426/PUP od 16. prosinca 2008. o jačanju Eurojusta i izmjeni Odluke 2002/187/PUP o osnivanju Eurojusta s ciljem jačanja borbe protiv teških kaznenih djela, SL 2009 L 138 (odluke o Eurojustu).

- poticanje i unapređivanje koordinacije istraga i progona među nadležnim tijelima različitih država članica,
- olakšavanje izvršavanja zahtjeva i odluka koji se odnose na pravosudnu suradnju.

Funkcije Eurojusta vrše nacionalni članovi. Svaka država članica imenuje po jednog suca ili tužitelja Eurojusta s potrebnim stručnim vještinama za izvršavanje zadaća potrebnih za poticanje i unapređenje pravosudne suradnje. Status tog suca ili tužitelja podliježe nacionalnom zakonodavstvu. Osim toga, nacionalni članovi zajednički su okupljeni u kolegij radi izvršavanja posebnih Eurojustovih zadaća.

Eurojust može obrađivati osobne podatke ako je to potrebno da bi ostvario svoje ciljeve. Međutim, ta je mogućnost ograničena na određene informacije u vezi s osobama osumnjičenima za počinjenje kaznenog djela ili sudjelovanje u njemu ili osobama osuđenima za kazneno djelo u nadležnosti Eurojusta. Eurojust može obrađivati i informacije u vezi sa svjedocima ili žrtvama kaznenih djela iz nadležnosti Eurojusta⁸³³. U iznimnim okolnostima i tijekom ograničenog vremenskog razdoblja Eurojust može obrađivati širi raspon osobnih podataka u vezi s okolnostima kaznenog djela ako se takvi podaci neposredno odnose na istragu u tijeku. Unutar svojeg područja nadležnosti Eurojust može surađivati s drugim institucijama, tijelima i agencijama Europske unije i s njima razmjenjivati osobne podatke. Eurojust može surađivati i razmjenjivati podatke i s trećim zemljama i organizacijama.

U vezi sa zaštitom podataka, Eurojust mora jamčiti razinu zaštite barem jednaku načelima iz modernizirane Konvencije br. 108 i njezinim kasnijim izmjenama. Pri razmjeni podataka moraju se poštovati posebna pravila i ograničenja uvedena sporazumom o suradnji ili radnim dogovorom u skladu s Odlukama Vijeća o Eurojustu i Pravilima o zaštiti podataka u Eurojustu⁸³⁴.

U okviru Eurojusta osnovano je Zajedničko nadzorno tijelo (JSB) sa zadaćom nadzora obrade osobnih podataka koju provodi Eurojust. Pojedinci se mogu žaliti Zajedničkom nadzornom tijelu ako nisu zadovoljni Eurojustovom odlukom u vezi sa zahtjevom za pristup, ispravak, blokiranje ili brisanje osobnih podataka. Ako Eurojust takve osobne podatke obrađuje nezakonito, snosi odgovornost u skladu s nacionalnim zakonodavstvom države članice u mjestu njegova sjedišta, Nizozemskoj, za štetu prouzročenu ispitaniku.

833 Pročišćena verzija Odluke Vijeća 2002/187/PUP kako je izmijenjena Odlukom Vijeća 2003/659/PUP i Odlukom Vijeća 2009/426/PUP, članak 15. stavak 2.

834 Poslovnik o obradi i zaštiti osobnih podataka u Eurojustu, SL 2005 C 68/01, 19. ožujka 2005., str. 1.

Izgledi

Europska komisija iznijela je prijedlog uredbe o reformi Eurojusta u srpnju 2013. Prijedlog je bio dopunjen prijedlogom o uspostavljanju Ureda europskog javnog tužitelja (vidjeti dalje u tekstu). Tom se uredbom nastoje pojednostaviti funkcije i struktura kako bi bile u skladu s Lisabonskim ugovorom. Nadalje, cilj je reforme uspostaviti jasnu podjelu između operativnih zadaća Eurojusta, koje obavlja njegov Kolegij, te njegovih administrativnih zadaća. Time će se i državama članicama omogućiti da se više posvete operativnim zadaćama. Osnovat će se novi Izvršni odbor koji će pomagati Kolegiju u obavljanju administrativnih zadaća⁸³⁵.

Ured europskog javnog tužitelja

Države članice imaju isključivu nadležnost nad progonom kaznenih djela prijevare i nepravilne primjene proračuna EU-a, koja mogu imati i prekogranične posljedice. Raste važnost istrage, kaznenog progona i podizanja optužnice protiv počinitelja takvih kaznenih djela, posebice s obzirom na trenutačnu gospodarsku krizu⁸³⁶. Europska komisija donijela je prijedlog Uredbe o osnivanju neovisnog Ureda europskog javnog tužitelja (EPPO)⁸³⁷ s ciljem borbe protiv kaznenih djela koja utječu na financijske interese EU-a. EPPO će se osnovati u sklopu postupka pojačane suradnje, koji omogućuje da najmanje devet država članica uspostavi naprednu razinu suradnje unutar struktura EU-a bez uključivanja ostalih zemalja EU-a⁸³⁸. Belgija, Bugarska, Cipar, Češka, Estonija, Finska, Francuska, Grčka, Hrvatska, Latvija, Litva, Luksemburg, Njemačka, Portugal, Rumunjska, Slovačka, Slovenija i Španjolska pridružile su se pojačanoj suradnji, a Austrija i Italija izrazile su namjeru pridruživanja⁸³⁹.

EPPO će biti nadležan za istragu i progon kaznenih djela prijevare i drugih kaznenih djela u EU-u koja utječu na financijske interese EU-a, s ciljem učinkovite koordinacije

835 Vidjeti internetsku stranicu Komisije posvećenu Eurojustu.

836 Vidjeti Europska komisija (2013.), Prijedlog uredbe Vijeća o osnivanju Ureda europskog javnog tužitelja, COM(2013) 534 final, Bruxelles, 17. srpnja 2013., str. 1. i internetsku stranicu Komisije posvećenu EPPO-u.

837 Europska komisija (2013.), Prijedlog uredbe Vijeća o osnivanju Ureda europskog javnog tužitelja, COM(2013) 534 final, Bruxelles, 17. srpnja 2013.

838 Ugovor o funkcioniranju Europske unije, članak 86. stavak 1. i članak 329. stavak 1.

839 Vidjeti Vijeće Europske unije (2017.), „*Postignut dogovor 20 država članica o pojedinostima uspostave Ureda europskog javnog tužitelja*“, priopćenje za medije, 8. lipnja 2017.

istraga i progona neovisno o nacionalnim pravnim porecima te s ciljem poboljšanja iskorištavanja resursa i razmjene informacija na europskoj razini⁸⁴⁰.

EPPO će predvoditi europski javni tužitelj i najmanje po jedan imenovani europski tužitelj u svakoj državi članici zadužen za provođenje istraga i progona u toj državi članici.

U Prijedlogu se utvrđuju snažne zaštitne mjere kojima se jamče prava osoba uključених u istrage EPPO-a kako su propisana nacionalnim zakonodavstvom, pravom EU-a i Poveljom EU-a o temeljnim pravima. Za istražne mjere koje se uglavnom odnose na temeljna prava bit će potrebno prethodno odobrenje nacionalnog suda⁸⁴¹. Istrage EPPO-a podlijegat će sudskom preispitivanju nacionalnih sudova⁸⁴².

Na obradu administrativnih osobnih podataka koju vrši EPPO primjenjivat će se Uredba o zaštiti podataka u institucijama Europske unije⁸⁴³. Za obradu osobnih podataka u vezi s operativnim pitanjima, kao što je Europol, EPPO će imati zaseban sustav zaštite podataka sličan onome kojim se uređuju aktivnosti Europolu i Eurojusta, s obzirom na to da će izvršavanje funkcija EPPO-a uključivati obradu osobnih podataka s tijelima za izvršavanje zakonodavstva i progon na razini država članica. Pravila EPPO-a za zaštitu podataka stoga su gotovo jednaka odredbama Direktive o zaštiti podataka za policiju i tijela kaznenog pravosuđa. Prema Prijedlogu o osnivanju EPPO-a, obrada osobnih podataka mora biti u skladu s načelima zakonitosti i pravednosti, ograničenja svrhe, smanjenja količine podataka, točnosti, cjelovitosti i povjerljivosti. EPPO mora, koliko je to moguće, jasno razlikovati osobne podatke različitih vrsta ispitanika, kao što su osobe osuđene za kaznena djela, osobe koje su samo osumnjičene, žrtve i svjedoci. Također mora nastojati provjeriti kvalitetu obrađenih osobnih podataka i razlikovati, koliko je to moguće, osobne podatke na temelju činjenica iz osobnih podataka i na temelju osobnih procjena.

Prijedlog sadržava odredbe o pravima ispitanika, točnije pravima na informacije, pristup vlastitim osobnim podacima te na ispravak, brisanje i ograničenje obrade, te se

840 Europska komisija (2013.), Prijedlog uredbe Vijeća o osnivanju Ureda europskog javnog tužitelja, COM(2013) 534 final, Bruxelles, 17. srpnja 2013., str. 1. i str. 50.-51. Vidjeti i [internetsku stranicu Komisije posvećenu EPPO-u](#).

841 Europska komisija (2013.), Prijedlog uredbe Vijeća o osnivanju Ureda europskog javnog tužitelja, COM(2013) 534 final, Bruxelles, 17. srpnja 2013., članak 26. stavak 4.

842 *Ibid.*, članak 36.

843 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

njime utvrđuje da se takva prava mogu ostvarivati i neizravno, putem EDPS-a. Prijedlog također utjelovljuje načela sigurnosti obrade i odgovornosti, kojima se uvjetuje da EPPO provede odgovarajuće tehničke i organizacijske mjere kako bi osigurao razinu sigurnosti koja odgovara rizicima obrade, vodi evidenciju o svim aktivnostima obrade i provodi procjene učinka zaštite podataka prije same obrade ako postoji vjerojatnost da će neka vrsta obrade (primjerice, obrada koja uključuje nove tehnologije) uzrokovati visok rizik za prava pojedinaca. Naposljetku, Prijedlogom se predviđa da Kolegij imenuje službenika za zaštitu podataka koji mora biti uključen u sva pitanja u vezi sa zaštitom osobnih podataka i koji mora osigurati postupanje EPPO-a u skladu sa svim mjerodavnim zakonodavstvom o zaštiti podataka.

8.3.2. Zaštita podataka u zajedničkim informacijskim sustavima na razini Europske unije

Osim razmjene podataka među državama članicama i osnivanja specijaliziranih tijela Europske unije za suzbijanje prekograničnog kriminala, kao što su Europol, Eurojust i EPPO, na razini Europske unije uspostavljeno je nekoliko zajedničkih informacijskih sustava koji omogućuju i olakšavaju suradnju i razmjenu podataka između nadležnih nacionalnih tijela i tijela EU-a u posebne svrhe u područjima zaštite granica, imigracija i azila te carine. Kako je schengensko područje prvotno uspostavljeno međunarodnim sporazumom neovisnim o pravu EU-a, tako je i Schengenski informacijski sustav (SIS) izrastao iz multilateralnih sporazuma te je naknadno obuhvaćen pravom EU-a. Vizni informacijski sustav (VIS), Eurodac, Eurosur i carinski informacijski sustav (CIS) nastali su kao instrumenti uređeni pravom EU-a.

Nadzor nad tim sustavima zajednički provode nacionalna nadzorna tijela i EDPS. Kako bi se osigurala visoka razina zaštite, ta tijela surađuju u okviru koordinacijskih skupina za nadzor (SCG-a), što se odnosi na sljedeće opsežne informacijske sustave: 1) Eurodac; 2) vizni informacijski sustav; 3) Schengenski informacijski sustav; 4) carinski informacijski sustav; i 5) informacijski sustav unutarnjeg tržišta⁸⁴⁴. SCG-ovi obično se sastaju dvaput godišnje, pod nadležnošću odabranog predsjednika, i donose smjernice, raspravljaju o prekograničnim predmetima ili donose zajedničke okvire za inspekcije.

⁸⁴⁴ Vidjeti [internetsku stranicu o koordiniranju nadzora](#) Europskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

Europska agencija za opsežne informacijske sustave (eu-LISA)⁸⁴⁵, osnovana 2012., odgovorna je za operativno upravljanje Schengenskim informacijskim sustavom druge generacije (SIS II), viznim informacijskim sustavom (VIS) i Eurodacom. Osnovna je zadaća agencije eu-LISA osigurati učinkovit, siguran i neprekidan rad informacijskih sustava. Odgovorna je i za donošenje potrebnih mjera sigurnosti sustava i podataka.

Schengenski informacijski sustav

Godine 1985. nekoliko je država članica nekadašnje Europske zajednice sklopilo Sporazum s državama Ekonomske unije Beneluksa, Njemačkom i Francuskom o postupnom ukidanju kontrola na zajedničkim granicama (Schengenski sporazum) kako bi se stvorio prostor za slobodno kretanje osoba, neometan graničnim kontrolama unutar schengenskog prostora⁸⁴⁶. Kao protuteža prijetnji javnoj sigurnosti uslijed otvaranja granica, uspostavljene su pojačane granične kontrole na vanjskim granicama schengenskog prostora kao i uska suradnja nacionalne policije i pravosudnih tijela.

Budući da je Schengenskom sporazumu pristupilo još država, schengenski je sustav konačno integriran u pravni okvir Europske unije Ugovorom iz Amsterdama⁸⁴⁷. Ta je odluka provedena 1999. Najnovija verzija Schengenskog informacijskog sustava, takozvani SIS II, puštena je u rad 9. travnja 2013. Trenutačno se njime služi većina država članica EU-a⁸⁴⁸ te Island, Lihtenštajn, Norveška i Švicarska⁸⁴⁹. Europol i Eurojust također imaju pristup sustavu SIS II.

SIS II sastoji se od središnjeg sustava (C-SIS), nacionalnog sustava (N-SIS) u svakoj državi članici i komunikacijske infrastrukture između središnjeg sustava i nacionalnih sustava. C-SIS sadržava određene podatke o osobama i predmetima koje unose

845 Uredba (EU) br. 1077/2011 Europskog parlamenta i Vijeća od 25. listopada 2011. o osnivanju Europske agencije za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde, SL 2011 L 286.

846 Sporazum između vlada država Ekonomske unije Beneluksa, Savezne Republike Njemačke i Francuske Republike o postupnom ukidanju kontrola na zajedničkim granicama, SL 2000 L 239.

847 Europske zajednice (1997.), Ugovor iz Amsterdama o izmjeni Ugovora o Europskoj uniji, ugovorâ o osnivanju Europskih zajednica i određenih s njima povezanih akata, SL 1997 C 340.

848 Hrvatska, Cipar i Irska provode pripremne aktivnosti za pristupanje sustavu SIS II, no još mu nisu pridružene. Vidjeti informacije o Schengenskom informacijskom sustavu dostupne na [internetskoj stranici Glavne uprave Europske komisije za migracije i unutarnje poslove](#).

849 Uredba (EZ) br. 1987/2006 Europskog parlamenta i Vijeća od 20. prosinca 2006. o uspostavi, djelovanju i korištenju druge generacije Schengenskog informacijskog sustava, SL 2006 L 381 (SIS II), i Vijeće Europske unije (2007.), Odluka Vijeća 2007/533/PUP od 12. lipnja 2007. o osnivanju, radu i korištenju druge generacije Schengenskog informacijskog sustava (SIS II), SL 2007 L 205.

države članice. SIS-om se služe nacionalna tijela za graničnu kontrolu te policijska, carinska, vizna i pravosudna tijela diljem schengenskog prostora. Svaka od država članica upravlja nacionalnom kopijom sustava C-SIS, poznatom kao nacionalni Schengenski informacijski sustav (N-SIS) koji se neprestano ažurira, čime se ažurira i C-SIS. U SIS-u postoje različite vrste upozorenja:

- osoba nema pravo ući u schengenski prostor ili ostati u njemu,
- osobu ili predmet traže pravosudna tijela ili tijela za izvršavanje zakonodavstva (npr. europski uhiđbeni nalozi, zahtjevi za skrivene provjere),
- osoba je prijavljena kao nestala, ili
- roba, poput novčanica, automobila, kamiona, vatrenog oružja i identifikacijskih dokumenata, prijavljena je kao ukradena ili izgubljena imovina.

U slučaju upozorenja treba pokrenuti prateće aktivnosti putem ureda SIRENE. SIS II ima nove funkcionalnosti kao što je mogućnost unosa: biometrijskih podataka, poput otisaka prstiju i fotografija; novih vrsta upozorenja, poput ukradenih plovila, zrakoplova, spremnika ili sredstava plaćanja; pojačanih upozorenja o osobama i predmetima; kopija europskih uhiđbenih naloga (EAW-ova) o osobama traženima radi uhićenja, predaje ili izručenja.

SIS II temelji se na dvama aktima koji se međusobno nadopunjuju: Odluci o sustavu SIS II⁸⁵⁰ i Uredbi o sustavu SIS II⁸⁵¹. Zakonodavac EU-a primjenjivao je različite pravne osnove za donošenje Odluke i Uredbe. Odlukom se uređuje upotreba sustava SIS II u svrhe obuhvaćene suradnjom policije i pravosudnih tijela u kaznenim predmetima (nekadašnji treći stup EU-a). Uredba se primjenjuje na postupke upozorenja koji potpadaju pod politike viza, azila, imigracija i druge politike koje se odnose na slobodno kretanje osoba (nekadašnji prvi stup). Postupci upozorenja za svaki stup trebali su se regulirati zasebnim aktima s obzirom na to da su navedena dva pravna akta done-sena prije Ugovora iz Lisabona i ukidanja strukture stupova.

850 Odluka Vijeća 2007/533/PUP od 12. lipnja 2007. o osnivanju, radu i korištenju druge generacije Schengenskog informacijskog sustava (SIS II), SL L 205, 7. kolovoza 2007.

851 Uredba (EZ) br. 1987/2006 Europskog parlamenta i Vijeća od 20. prosinca 2006. o uspostavi, djelovanju i korištenju druge generacije Schengenskog informacijskog sustava (SIS II), SL L 381, 28. prosinca 2006.

Oba pravna akta sadrže odredbe o zaštiti podataka. Odlukom o sustavu SIS II zabranjuje se obrada „posebnih kategorija podataka”⁸⁵². Obrada osobnih podataka obuhvaćena je moderniziranom Konvencijom br. 108⁸⁵³. Usto, osobe imaju pravo na pristup osobnim podacima koji se odnose na njih, a koji se unesu u SIS II⁸⁵⁴.

Uredbom o sustavu SIS II reguliraju se uvjeti i postupci za unošenje i obradu upozorenja u vezi s uskraćivanjem ulaska ili boravka osoba koje nisu građani EU-a. Njome se također propisuju pravila za razmjenu dopunskih i dodatnih informacija u svrhu ulaska u državu članicu ili boravka u njoj⁸⁵⁵. Uredba sadržava i odredbe o zaštiti podataka. Osjetljive kategorije podataka, utvrđene člankom 9. stavkom 1. Opće uredbe o zaštiti podataka, ne smiju se obrađivati⁸⁵⁶. Uredba o sustavu SIS II sadržava i određena prava za ispitanika, odnosno:

- pravo na pristup osobnim podacima koji se odnose na ispitanika⁸⁵⁷,
- pravo na ispravak netočnih podataka⁸⁵⁸,
- pravo na brisanje nezakonito pohranjenih podataka⁸⁵⁹, te
- pravo na informacije u slučaju izdanog upozorenja protiv ispitanika. Informacije se moraju pružiti u pisanom obliku i mora im se priložiti kopija ili pozivanje na nacionalnu odluku na temelju koje je izdano upozorenje⁸⁶⁰.

Pravo na informacije ne dodjeljuje se ako 1) osobni podaci nisu dobiveni od predmetnog ispitanika i pružanje informacija nije moguće ili bi zahtijevalo nerazmjeran napor, 2) ako ispitanik već raspolaže informacijama ili 3) ako se nacionalnim pravom omogućuje ograničenje na temelju, među ostalim, zaštite nacionalne sigurnosti ili sprečavanja kaznenih djela⁸⁶¹.

852 Odluka o sustavu SIS II, članak 56.; Uredba o sustavu SIS II, članak 40.

853 Odluka o sustavu SIS II, članak 57.

854 Odluka o sustavu SIS II, članak 58.; Uredba o sustavu SIS II, članak 41.

855 Uredba o sustavu SIS II, članak 2.

856 *Ibid.*, članak 40.

857 *Ibid.*, članak 41. stavak 1.

858 *Ibid.*, članak 41. stavak 5.

859 *Ibid.*, članak 41. stavak 5.

860 *Ibid.*, članak 42. stavak 1.

861 *Ibid.*, članak 42. stavak 2.

Sukladno i Odluci o sustavu SIS II i Uredbi o sustavu SIS II, prava na pristup pojedinaca u vezi sa sustavom SIS II mogu se ostvariti u bilo kojoj državi članici te će se uređivati u skladu s nacionalnim zakonodavstvom te države članice⁸⁶².

Primjer: U predmetu *Dalea protiv Francuske*⁸⁶³ tužitelju je odbijen zahtjev za vizu radi posjeta Francuskoj jer su francuske vlasti prijavile Schengenskom informacijskom sustavu da mu se mora uskratiti ulazak u zemlju. Tužitelj je neuspješno tražio pristup i ispravljanje ili brisanje podataka pred francuskom Komisijom za zaštitu podataka i, konačno, pred Državnim vijećem. ESLJP je smatrao da je prijava tužitelja Schengenskom informacijskom sustavu bila u skladu sa zakonom i legitimnom svrhom zaštite nacionalne sigurnosti. Budući da tužitelj nije pokazao kako je zapravo bio oštećen uskratom ulaska u schengenski prostor i budući da su se primjenjivale odgovarajuće mjere kojima je bio zaštićen od proizvoljnih odluka, miješanje u njegovo pravo na poštovanje privatnog života bilo je razmjerno. Stoga je tužiteljeva pritužba na temelju članka 8. proglašena neprihvatljivom.

Nadležno nacionalno nadzorno tijelo u svakoj državi članici nadzire nacionalni sustav N-SIS. Nacionalno nadzorno tijelo mora osigurati da se revizija postupaka obrade podataka u sklopu nacionalnog sustava N-SIS provede barem jednom svake četiri godine⁸⁶⁴. Nacionalna nadzorna tijela i EDPS surađuju i osiguravaju koordinirani nadzor sustava N-SIS, a EDPS je odgovoran za nadzor sustava C-SIS. Radi transparentnosti, svake dvije godine Europskom parlamentu, Vijeću i agenciji eu-LISA šalje se zajedničko izvješće o aktivnostima. Koordinacijska skupina za nadzor sustava SIS II (SCG) utemeljena je kako bi se osigurala koordinacija nadzora SIS-a i sastaje se do dva puta godišnje. Skupinu čine EDPS i predstavnici nadzornih tijela država članica koje su uvele SIS II te Islanda, Lihtenštajna, Norveške i Švicarske jer se SIS primjenjuje i na njih jer su članice schengenskog sustava⁸⁶⁵. Cipar, Hrvatska i Irska još nisu članovi sustava SIS II, i stoga u SCG-u sudjeluju samo kao promatrači. U kontekstu SCG-a, EDPS i nacionalna nadzorna tijela aktivno surađuju tako što razmjenjuju informacije, pomažu si međusobno prilikom provođenja revizija i inspekcija, izrađuju nacрте usklađenih prijedloga za zajednička rješenja svih poteškoća i promoviraju svijest

⁸⁶² Uredba o sustavu SIS II, članak 41. stavak 1. i Odluka o sustavu SIS II, članak 58.

⁸⁶³ ESLJP, *Dalea protiv Francuske*, br. 964/07, 2. veljače 2010.

⁸⁶⁴ Uredba o sustavu SIS II, članak 60. stavak 2.

⁸⁶⁵ Vidjeti internetsku stranicu o Schengenskom informacijskom sustavu Europskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

o pravima na zaštitu podataka⁸⁶⁶. Skupina SCG za sustav SIS II također donosi smjernice kao pomoć ispitanicima. Jedan je od primjera vodič koji pomaže ispitanicima u ostvarivanju prava na pristup⁸⁶⁷.

Izgledi

Europska komisija provela je 2016. postupak ocjenjivanja sustava SIS⁸⁶⁸ koji je pokazao da su uspostavljeni nacionalni mehanizmi koji ispitanicima omogućuju pristup vlastitim osobnim podacima te njihov ispravak i brisanje u sustavu SIS II ili ostvarenje naknade u vezi s netočnim podacima. Kako bi se poboljšale učinkovitost i djelotvornost sustava SIS II, Europska komisija iznijela je tri prijedloga uredbi:

- Uredba o uspostavi, djelovanju i korištenju sustava SIS u području graničnih kontrola, kojom bi se izvan snage stavila Uredba o sustavu SIS II,
- Uredba o uspostavi, djelovanju i korištenju sustava SIS u području suradnje policije i pravosudnih tijela u kaznenim predmetima, kojom bi se, među ostalim, izvan snage stavila Odluka o sustavu SIS II, te
- Uredba o upotrebi sustava SIS za povratak državljana trećih zemalja koji nezakonito borave na nekom području.

Važno je napomenuti da se prijedlozima omogućuje obrada drugih kategorija biometrijskih podataka osim fotografija i otisaka prstiju, koji su već uključeni u postojeći sustav SIS II. Prikazi lica, otisci dlana i DNK profili također će se pohranjivati u bazi podataka SIS. Osim toga, Uredbom o sustavu SIS II i Odlukom o sustavu SIS II dopuštena je mogućnost pretraživanja otisaka prstiju radi identifikacije pojedinca, dok je prijedlozima ta pretraga učinjena obaveznom ako se identitet osobe ne može utvrditi na drugi način. Prikazi lica, fotografije i otisci dlanova primjenjivat će se za pretraživanje sustava i identifikaciju osoba kada to postane tehnički izvedivo. Nova pravila o biometrijskim karakteristikama uzrokuju posebne rizike za prava pojedinaca.

866 Uredba o sustavu SIS II, članak 46. i Odluka o sustavu SIS II, članak 62.

867 Vidjeti SCG za sustav SIS II, The Schengen Information System. A guide for exercising the right of access (Schengenski informacijski sustav – Vodič za ostvarivanje prava pristupa), dostupan na engleskom jeziku na internetskoj stranici EDPS-a.

868 Europska komisija (2016.), Izvješće Komisije Europskom parlamentu i Vijeću o ocjeni druge generacije Schengenskog informacijskog sustava (SIS II) u skladu s člankom 24. stavkom 5., člankom 43. stavkom 3. i člankom 50. stavkom 5. Uredbe (EZ) br. 1987/2006 te člankom 59. stavkom 3. i člankom 66. stavkom 5. Odluke 2007/533/PUP, COM(2016) 880 final, Bruxelles, 21. prosinca 2016.

U mišljenju o prijedlozima Komisije⁸⁶⁹ EDPS je istaknuo da su biometrijski podaci izuzetno osjetljivi te da se njihovo uvođenje u tako opsežnu bazu podataka treba temeljiti na procjeni potrebe za njihovim uvrštavanjem u SIS koja će se temeljiti na dokazima. Drugim riječima, potrebno je dokazati potrebu za obradom tih novih karakteristika. EDPS je također zaključio da je potrebno dodatno pojasniti koja se vrsta podataka može uvrstiti u DNK profil. Budući da DNK profil može sadržavati osjetljive podatke (najbolji bi primjer bili podaci koji otkrivaju zdravstvene probleme), DNK profili koji se pohranjuju u SIS-u trebaju sadržavati sljedeće: „samo najmanju količinu informacija koja je strogo nužna za identifikaciju nestalih osoba i koja ne sadržava izričite zdravstvene podatke, rasno podrijetlo i druge osjetljive podatke”⁸⁷⁰. Međutim, prijedlozima se uspostavljaju dodatne zaštitne mjere kojima se ograničavaju prikupljanje i daljnja obrada podataka na ono što je strogo nužno i operativno se zahtijeva, a pristup se ograničava na osobe koje imaju operativnu potrebu za obradom osobnih podataka⁸⁷¹. Prijedlozima se također ovlašćuje agenciju eu-LISA da redovito izrađuje izvješća o kvaliteti podataka za države članice kako bi se redovito preispitivala upozorenja i osigurala kvaliteta podataka⁸⁷².

Vizni informacijski sustav

Vizni informacijski sustav (VIS), kojim također upravlja eu-LISA, razvijen je kao podrška provedbi zajedničke vizne politike Europske unije⁸⁷³. Zahvaljujući sustavu VIS, države schengenskog prostora mogu razmjenjivati podatke o podnositeljima zahtjeva za vizu putem potpuno centraliziranog sustava koji povezuje konzulate i veleposlanstva schengenskih država u državama izvan Europske unije s vanjskim graničnim prijelazima svih schengenskih država. U VIS-u se obrađuju podaci u vezi

869 EDPS (2017.), Mišljenje Europskog nadzornika za zaštitu podataka o novoj pravnoj osnovi Schengenskog informacijskog sustava, Mišljenje 7/2017, 2. svibnja 2017.

870 *Ibid.*, st. 22.

871 Europska komisija (2016.), Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, izmjeni Uredbe (EU) br. 515/2014 i stavljanju izvan snage Uredbe (EZ) br. 1986/2006, Odluke Vijeća 2007/533/PUP i Odluke Komisije 2010/261/EU, COM(2016) 883 final, Bruxelles, 21. prosinca 2016.

872 *Ibid.*, str. 15.

873 Vijeće Europske unije (2004.), Odluka Vijeća 2004/512/EZ od 8. lipnja 2004. o uspostavi viznog informacijskog sustava (VIS), SL 2004 L 213; Uredba (EZ) br. 767/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak, SL 2008 L 218 (Uredba o VIS-u); Vijeće Europske unije (2008.), Odluka Vijeća 2008/633/PUP od 23. lipnja 2008. o pristupu određenih tijela država članica i Europolu viznom informacijskom sustavu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih kaznenih djela i ostalih teških kaznenih djela, SL 2008 L 218.

sa zahtjevima za vizama za kratkotrajni boravak ili za provozaom kroz schengenski prostor. Uz pomoć biometrijskih podataka, a ponajviše otisaka prstiju, sustav VIS pograničnim tijelima omogućuje da provjere je li osoba koja je predložila vizu njezin valjani nositelj kao i da identificiraju osobe bez ikakvih dokumenata ili s lažnim dokumentima.

Uredbom (EZ) br. 767/2008 Europskog parlamenta i Vijeća o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak (Uredbom o VIS-u) utvrđuju se uvjeti i postupci za prijenos osobnih podataka o prijavama za vize za kratkotrajni boravak. Njome se također uređuju odluke koje se donose o zahtjevima, uključujući odluke o poništavanju, oduzimanju ili produljenju vize⁸⁷⁴. Uredba o VIS-u uglavnom obuhvaća podatke o podnositelju zahtjeva, njegove vize, fotografije, otiske prstiju, veze s prethodnim zahtjevima i dokumentaciju o zahtjevima osoba koje su u njegovoj pratnji ili podatke o osobama koje su uputile poziv⁸⁷⁵. Pristup VIS-u radi unosa, izmjene ili brisanja podataka ograničen je isključivo na tijela nadležna za izdavanje viza, dok je pristup radi uvida u podatke osiguran tijelima nadležnima za izdavanje viza i onima nadležnima za kontrole na vanjskim graničnim prijelazima, imigracijske kontrole i azil.

U određenim uvjetima nacionalna nadležna policijska tijela i Europol mogu zatražiti pristup podacima unesenima u sustav VIS radi sprečavanja, otkrivanja i istrage terorističkih i kaznenih djela⁸⁷⁶. Budući da je VIS osmišljen kao instrument za potporu u provedbi zajedničke politike o vizama, kada bi se on pretvorio u alat za izvršavanje zakonodavstva, prekršilo bi se načelo ograničenja svrhe prema kojem se, kako je pojašnjeno u [poglavlju 3.2.](#), zahtijeva da se osobni podaci obrađuju isključivo u posebne, izričite i zakonite svrhe te da budu primjereni, relevantni i ne prekomjerni u odnosu na svrhe zbog kojih se obrađuju. Zbog toga nacionalnim tijelima za izvršavanje zakonodavstva i Europolu nije dopušten rutinski pristup bazi podataka VIS. Pristup se može odobriti isključivo za pojedinačne slučajeve i mora biti popraćen strogim zaštitnim mjerama. Uvjeti i zaštitne mjere za pristup i uvid tih tijela u VIS uređeni su Odlukom Vijeća 2008/633/PUP⁸⁷⁷.

874 Uredba o VIS-u, članak 1.

875 Članak 5. Uredbe (EZ) br. 767/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o viznom informacijskom sustavu (VIS) i razmjeni podataka među državama članicama o vizama za kratkotrajni boravak (Uredba o VIS-u), SL 2008 L 218.

876 Vijeće Europske unije (2008.), Odluka Vijeća 2008/633/PUP od 23. lipnja 2008. o pristupu određenih tijela država članica i Eurola viznom informacijskom sustavu (VIS) za traženje podataka u svrhu sprečavanja, otkrivanja i istraga terorističkih kaznenih djela i ostalih teških kaznenih djela, SL 2008 L 218.

877 *Ibid.*

Uredbom o VIS-u utvrđuju se i prava ispitanika. Ta su prava sljedeća:

- pravo na dobivanje informacija od nadležne države članice o identitetu i kontaktnim podacima voditelja obrade podataka koji je zadužen za obradu osobnih podataka u toj državi članici, svrhama zbog kojih se podaci obrađuju unutar VIS-a, kategorijama osoba kojima se podaci mogu prenositi (primateljima) te o rokovima čuvanja podataka. Podnositelji zahtjeva za vizu također moraju biti obaviješteni o tome da je prikupljanje njihovih osobnih podataka za VIS obvezno za preispitivanje njihova zahtjeva, a države članice moraju ih obavijestiti i o postojanju prava na pristup vlastitim podacima i prava da se zatraži njihovo ispravljanje ili brisanje te o postupcima putem kojih mogu ostvariti ta prava⁸⁷⁸,
- pravo na pristup osobnim podacima koji se odnose na njih, a koji su zabilježeni u VIS-u⁸⁷⁹,
- pravo na ispravak netočnih podataka⁸⁸⁰,
- pravo na brisanje nezakonito pohranjenih podataka⁸⁸¹.

Da bi se osigurao nadzor sustava VIS, osnovana je Koordinacijska skupina za nadzor (SCG) sustava VIS. Čine je predstavnici EDPS-a i nacionalnih nadzornih tijela koji se sastaju dva puta godišnje. Skupinu čine predstavnici 28 država članica EU-a te Islanda, Lihtenštajna, Norveške i Švicarske.

Eurodac

Eurodac označava europski daktiloskopski sustav⁸⁸². Radi se o centraliziranom sustavu s podacima o otiscima prstiju državljana trećih zemalja i osoba bez

878 Uredba o VIS-u, članak 37.

879 *Ibid.*, članak 38. stavak 1.

880 *Ibid.*, članak 38. stavak 2.

881 *Ibid.*

882 Vidjeti [internetsku stranicu o Eurodacu](#) Europskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

državljanstva koji traže azil u jednoj od država članica Europske unije⁸⁸³. Sustav se upotrebljava od siječnja 2003., kada je donesena Uredba Vijeća (EZ) br. 2725/2000., čija je preinaka stupila na snagu 2015. Njegova je svrha prvenstvo da pomaže prilikom utvrđivanja koja bi država članica trebala biti odgovorna za razmatranje određenog zahtjeva za azil prema Uredbi Vijeća (EZ) br. 604/2013. Tom se Uredbom utvrđuju kriteriji i mehanizmi za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva (Uredba Dublin III)⁸⁸⁴. Osobni podaci u Eurodacu uglavnom služe omogućivanju primjene Uredbe Dublin III⁸⁸⁵.

Nacionalna tijela za izvršavanje zakonodavstva i Europol smiju uspoređivati otiske prstiju koji se povezuju s kaznenim istragama s otiscima prstiju u Eurodacu, no samo u svrhu sprečavanja, otkrivanja ili istrage terorističkih i drugih teških kaznenih djela. Budući da je Eurodac osmišljen kao instrument za pružanje potpore u provedbi politike EU-a o azilu, a ne kao alat za izvršavanje zakonodavstva, tijela za izvršavanje zakonodavstva imaju pravo pristupa bazi podataka samo u određenim slučajevima, u određenim okolnostima i pod određenim uvjetima⁸⁸⁶. Za daljnju uporabu podataka u svrhu izvršavanja zakonodavstva primjenjuje se Direktiva o zaštiti podataka za policiju i tijela kaznenog pravosuđa, a podaci koji se upotrebljavaju u osnovnu svrhu pomaganja u provedbi Uredbe Dublin III. zaštićeni su Općom uredbom o zaštiti podataka. Zabranjen je daljnji prijenos osobnih podataka koje prikupi država članica ili Europol u skladu s preinačenom Uredbom o Eurodacu bilo kojoj trećoj zemlji, međunarodnoj organizaciji ili privatnom subjektu s nastanom u EU-u ili izvan njega⁸⁸⁷.

883 Uredba Vijeća (EZ) br. 2725/2000 od 11. prosinca 2000. o osnivanju sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu Dublinske konvencije, SL 2000 L 316; Uredba Vijeća (EZ) br. 407/2002 od 28. veljače 2002. o utvrđivanju određenih pravila za provedbu Uredbe (EZ) br. 2725/2000 o osnivanju sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu Dublinske konvencije, SL 2002 L 62 (uredbe o Eurodacu), Uredba (EU) br. 603/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o uspostavi sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu Uredbe (EU) br. 604/2013 o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva i o zahtjevima za usporedbu s podacima iz Eurodaca od strane tijela kaznenog progona država članica i Eurolpa u svrhu kaznenog progona te o izmjeni Uredbe (EU) br. 1077/2011 o osnivanju Europske agencije za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde, SL 2013 L 180, str. 1. (preinačena Uredba o Eurodacu).

884 Uredba (EU) br. 604/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva, SL 2013 L 180 (Uredba Dublin III).

885 Preinačena Uredba o Eurodacu, SL 2013 L 180, str. 1., članak 1. stavak 1.

886 *Ibid.*, članak 1. stavak 2.

887 *Ibid.*, članak 35.

Sustav Eurodac sastoji se od središnje jedinice, kojom upravlja eu-LISA, za pohranu i usporedbu otisaka prstiju i sustava za elektronički prijenos podataka među državama članicama i središnjom bazom podataka. Države članice uzimaju i prenose otiske prstiju svake osobe u dobi od najmanje 14 godina koja zatraži azil na njihovu državnom području te svake osobe koja nije državljanin Europske unije ili osobe bez državljanstva u dobi od najmanje 14 godina koja je uhićena zbog neovlaštenog prelaska njihove vanjske granice. Države članice također mogu uzeti i prenijeti otiske prstiju osoba koje nisu državljani Europske unije ili osoba bez državljanstva koje borave unutar njihova državnog područja bez dozvole.

Iako države članice mogu pristupiti Eurodacu i zatražiti usporedbe s podacima o otiscima prstiju, samo ona država članica koja je prikupila te otiske i prenijela ih središnjoj jedinici ima pravo izmijeniti podatke ispravljanjem, dopunom ili brisanjem tih podataka⁸⁸⁸. Agencija eu-LISA vodi evidenciju o svim aktivnostima obrade podataka radi praćenja zaštite podataka i osiguravanja njihove sigurnosti⁸⁸⁹. Nacionalna nadzorna tijela pomažu ispitanicima i savjetuju ih o ostvarivanju njihovih prava⁸⁹⁰. Prikupljanje i prijenos podataka o otiscima prstiju podliježu sudskom preispitivanju nacionalnih sudova⁸⁹¹. Uredba o zaštiti podataka u institucijama Europske unije⁸⁹² i nadzor EDPS-a primjenjuju se na aktivnosti obrade središnjeg sustava, kojim upravlja eu-LISA u pogledu Eurodaca⁸⁹³. Ako je osoba pretrpjela štetu zbog nezakonitog postupka obrade ili drugog djelovanja koje nije u skladu s Uredbom o Eurodacu, ima pravo primiti naknadu štete od države članice odgovorne za pretrpljenu štetu⁸⁹⁴. Međutim, valja napomenuti kako su tražitelji azila posebno osjetljiva skupina ljudi koji često prelaze dug i opasan put. Zbog njihove osjetljivosti i neizvjesne situacije u kojoj se često nalaze tijekom postupka preispitivanja njihova zahtjeva za azil, ostvarenje njihovih prava, uključujući pravo na naknadu štete, u praksi može biti otežano.

Da bi se Eurodac upotrebljavao u svrhe izvršavanja zakonodavstva, države članice moraju imenovati tijela koja će imati pravo zatražiti pristup Eurodacu te tijela koja

888 *Ibid.*, članak 27.

889 *Ibid.*, članak 28.

890 *Ibid.*, članak 29.

891 *Ibid.*

892 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

893 Preinačena Uredba o Eurodacu, SL 2013 L 180, str. 1., članak 31.

894 *Ibid.*, članak 37.

će provjeravati jesu li zahtjevi za usporedbu zakoniti⁸⁹⁵. Pristup nacionalnih tijela i Europolu podacima o otiscima prstiju iz Eurodaca podliježu vrlo strogim uvjetima. Tijelo koje upućuje zahtjev mora podnijeti obrazloženi elektronički zahtjev tek nakon usporedbe podataka s podacima iz drugih dostupnih informacijskih sustava, kao što su nacionalne baze podataka o otiscima prstiju i VIS. Mora postojati prevladavajući rizik za javnu sigurnost koji usporedbu čini razmjernom. Usporedba mora biti doista nužna, mora se odnositi na određeni slučaj i moraju postojati opravdani razlozi za vjerovanje da bi ta usporedba značajno doprinijela sprečavanju, otkrivanju ili istrazi bilo kojih kaznenih djela o kojima je riječ, posebice kada postoji potkrijepljena sumnja da osumnjičenik, počinitelj kaznenog djela ili žrtva terorističkog kaznenog djela ili drugog teškog kaznenog djela pripada kategoriji koja podliježe prikupljanju otisaka prstiju u sklopu sustava Eurodac. Usporedba se mora izvršiti isključivo nad podacima o otiscima prstiju. Europol također mora ishoditi odobrenje države članice koja je te podatke o otiscima prstiju prikupila.

Osobni podaci pohranjeni u sustavu Eurodac koji se odnose na tražitelje azila čuvaju se 10 godina od datuma uzimanja otisaka prstiju, osim ako ispitanik dobije državljanstvo neke države članice Europske unije. U tom se slučaju podaci moraju odmah izbrisati. Podaci koji se odnose na strane državljane uhićene zbog nezakonitog prelaska vanjske granice čuvaju se 18 mjeseci. Ti se podaci moraju izbrisati čim ispitanik dobije dozvolu boravka, napusti područje Europske unije ili dobije državljanstvo neke države članice. Podaci o osobama kojima je odobren azil ostaju dostupni tri godine radi usporedbe u kontekstu sprečavanja, otkrivanja i istrage terorističkih i drugih teških kaznenih djela.

Osim svih država članica EU-a, na temelju međunarodnih sporazuma sustavom Eurodac služe se i Island, Norveška, Lihtenštajn i Švicarska.

Koordinacijska skupina za nadzor (SCG) Eurodaca uspostavljena je kako bi se osigurao nadzor sustava Eurodac. Čine je predstavnici EDPS-a i nacionalnih nadzornih tijela koji se sastaju dva puta godišnje. Skupinu čine predstavnici 28 država članica EU-a te Islanda, Lihtenštajna, Norveške i Švicarske⁸⁹⁶.

895 Roots, L. (2015.), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination” („Nova Uredba o EURODAC-u: otisci prstiju kao izvor neformalne diskriminacije”), *Baltic Journal of European Studies*, Tallinn University of Technology, sv. 5, br. 2, str. 108.–129.

896 Vidjeti [internetsku stranicu o Eurodacu](#) Europskog nadzornika za zaštitu podataka (dostupnu na engleskom jeziku).

Izgledi

U svibnju 2016. Komisija je izdala Prijedlog nove preinake Uredbe o Eurodacu u okviru reforme kojom se nastojalo poboljšati funkcioniranje Zajedničkog europskog sustava azila (CEAS)⁸⁹⁷. Predložena je preinaka važna jer će se njome znatno proširiti područje primjene originalne baze podataka Eurodac. Eurodac je prvotno stvoren radi pružanja potpore u provedbi CEAS-a pružanjem dokaza o otiscima prstiju kako bi se omogućilo određivanje države članice koja je odgovorna za razmatranje zahtjeva za azil podnesenog u EU-u. Predloženom preinakom proširit će se opseg baze podataka kako bi se olakšao povratak nezakonitih migranata⁸⁹⁸. Nacionalna tijela imat će uvid u bazu podataka u svrhu otkrivanja državljana trećih zemalja koji nezakonito borave u EU-u ili koji su nezakonito ušli u EU, kako bi prikupila dokaze koji će državama članicama pomoći da ih vrate u njihove zemlje. Usto, pravnim sustavom koji je trenutačno na snazi zahtijevaju se samo prikupljanje i pohrana otisaka prstiju, dok se u Prijedlogu uvodi prikupljanje prikaza lica pojedinaca⁸⁹⁹, što predstavlja drugu vrstu biometrijskih podataka. Prijedlogom bi se također smanjila minimalna dob djece od koje se smiju uzimati biometrijski podaci, na šest⁹⁰⁰ umjesto 14 godina, što je dobna granica prema Uredbi iz 2013. Prošireno područje primjene Prijedloga podrazumijeva da će ono predstavljati miješanje u prava na privatnost i zaštitu podataka većeg broja pojedinaca koji bi mogli biti uvršteni u bazu podataka. Kao protuteža tom miješanju, Prijedlogom i izmjenama i dopunama koje predlaže Odbor LIBE Europskog

897 Europska komisija, Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva] radi identificiranja državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom i o zahtjevima za usporedbu s podacima iz Eurodaca od strane tijela kaznenog progona država članica i Europolu u svrhu kaznenog progona (preinaka), COM(2016) 272 final, 4. svibnja 2016.

898 Vidjeti Memorandum s objašnjenjima o prijedlogu, str. 3.

899 Europska komisija, Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljanin treće zemlje ili osoba bez državljanstva] radi identificiranja državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom i o zahtjevima za usporedbu s podacima iz Eurodaca od strane tijela kaznenog progona država članica i Europolu u svrhu kaznenog progona (preinaka), COM(2016) 272 final, 4. svibnja 2016., članak 2. stavak 1.

900 *Ibid.*, članak 2. stavak 2.

parlamenta⁹⁰¹ nastoje se ojačati zahtjevi u pogledu zaštite podataka. U vrijeme izrade ovog priručnika rasprave o prijedlogu u Parlamentu i Vijeću još su bile u tijeku.

Eurosur

Europski sustav za nadzor granica (Eurosur)⁹⁰² osmišljen je kako bi pojačao kontrolu vanjskih granica schengenskog prostora otkrivanjem, sprečavanjem i suzbijanjem nezakonite imigracije i prekograničnog kriminala. On služi za poboljšanje razmjene informacija i operativne suradnje između nacionalnih koordinacijskih centara i agencije Frontex, agencije Europske unije koja je zadužena za razvijanje i primjenu novog koncepta integriranog upravljanja granicama⁹⁰³. Njegovi su opći ciljevi:

- smanjiti broj nezakonitih migranata koji neotkriveni ulaze u Europsku uniju,
- smanjiti broj smrti nezakonitih migranata spašavanjem većeg broja ljudi na moru,
- povećati unutarnju sigurnost EU-a u cjelini pomažući u sprečavanju prekograničnog kriminala⁹⁰⁴.

Eurosur je s radom započeo 2. prosinca 2013. u svim državama članicama s vanjskim granicama, a 1. prosinca 2014. i u ostalima. Uredba se primjenjuje na nadzor vanjskih kopnenih, morskih i zračnih granica država članica. Eurosur razmjenjuje i obrađuje osobne podatke u vrlo ograničenom opsegu s obzirom na to da države članice i Frontex smiju razmjenjivati samo identifikacijske brojeve brodova. Eurosur razmjenjuje

901 Europski parlament, [Izvješće](#) o Prijedlogu uredbe Europskog parlamenta i Vijeća o uspostavi sustava „Eurodac“ za usporedbu otisaka prstiju za učinkovitu primjenu [Uredbe (EU) br. 604/2013 o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za međunarodnu zaštitu koji je u jednoj od država članica podnio državljani treće zemlje ili osoba bez državljanstva] radi identifikiranja državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom i o zahtjevima za usporedbu s podacima iz Eurodaca od strane tijela kaznenog progona država članica i Europla u svrhu kaznenog progona (preinaka), PE 597.620v03-00, 9. lipnja 2017.

902 Uredba (EU) br. 1052/2013 Europskog parlamenta i Vijeća od 22. listopada 2013. o uspostavi Europskog sustava nadzora granica (EUROSUR), SL 2013 L 295.

903 Uredba (EU) br. 2016/1624 Europskog parlamenta i Vijeća od 14. rujna 2016. o europskoj graničnoj i obalnoj straži i o izmjeni Uredbe (EU) 2016/399 Europskog parlamenta i Vijeća te o stavljanju izvan snage Uredbe (EZ) br. 863/2007 Europskog parlamenta i Vijeća, Uredbe Vijeća (EZ) br. 2007/2004 i Odluke Vijeća 2005/267/EZ, SL L 251.

904 Vidjeti i: Europska komisija (2008.), Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija: Razmatranje uspostave Europskog sustava za nadzor granica (Eurosur), COM(2008) 68 final, Bruxelles, 13. veljače 2008.; Europska komisija (2011.), Procjena učinka uz Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi Europskog sustava za nadzor granica (Eurosur), radni dokument osoblja, SEC(2011) 1536 final, Bruxelles, 12. prosinca 2011, str. 18.

operativne informacije, poput lokacije patrola i incidenata, a opće je pravilo da informacije koje se razmjenjuju ne smiju sadržavati osobne podatke⁹⁰⁵. U iznimnim slučajevima u kojima se u okviru Eurosur razmjenjuju osobni podaci Uredbom je utvrđeno da se primjenjuje opći pravni okvir EU-a za zaštitu podataka⁹⁰⁶.

Eurosur stoga osigurava pravo na zaštitu podataka, prvenstveno tako što zahtijeva da su razmjene osobnih podataka u skladu s kriterijima i zaštitnim mjerama koji su uspostavljeni Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa i Općom uredbom o zaštiti podataka⁹⁰⁷.

Carinski informacijski sustav

Drugi važan informacijski sustav uspostavljen na razini EU-a jest carinski informacijski sustav (CIS)⁹⁰⁸. Tijekom uspostave unutarnjeg tržišta ukinute su sve kontrole i formalnosti povezane s robom koja se kreće unutar područja EU-a, što je povećalo rizik od prijevare. Protuteža tom riziku pojačana je suradnja među carinskim upravama država članica. Svrha je CIS-a pomoći državama članicama u sprečavanju, istrazi i progonu teških kršenja carinskih i poljoprivrednih zakona na razini država i EU-a. CIS je osnovan dvama pravnim aktima koji su doneseni na različitim pravnim osnovama: Uredba Vijeća (EZ) br. 515/97 odnosi se na suradnju različitih nacionalnih upravnih tijela radi suzbijanja prijevara u kontekstu carinske unije i zajedničke poljoprivredne politike, a Odlukom Vijeća 2009/917/PUP nastoji se pomoći u sprečavanju, istrazi i progonu teških kršenja carinskih zakona. To znači da se CIS ne odnosi samo na izvršavanje zakonodavstva.

Informacije iz CIS-a obuhvaćaju osobne podatke koji se odnose na zadržane, oduzete ili zaplijenjene proizvode, prijevozna sredstva, poduzeća, osobe, robu i gotovinu. Kategorije podataka koji se mogu obrađivati jasno su određene, a uključuju imena, državljanstvo, spol, datum i mjesto rođenja dotičnih osoba, razlog uvrštavanja

905 Europska komisija, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell* (EUROSUR: zaštita vanjskih granica schengenskog prostora – zaštita života migranata), 29. studenoga 2013.

906 Uredba (EU) br. 1052/2013, uvodna izjava 13. i članak 13.

907 *Ibid.*

908 Vijeće Europske unije (1995.), Akt Vijeća od 26. srpnja 1995. o sastavljanju Konvencije o uporabi informacijske tehnologije u carinske svrhe, SL 1995 C 316, koju je izmijenilo Vijeće Europske unije (2009.), Uredba br. 515/97 od 13. ožujka 1997. o uzajamnoj pomoći upravnih tijela država članica i o suradnji potonjih s Komisijom radi osiguravanja pravilne primjene propisa o carinskim i poljoprivrednim pitanjima, Odluka Vijeća 2009/917/PUP od 30. studenoga 2009. o uporabi informacijskih tehnologija u carinske svrhe, SL 2009 L 323 (Odluka o CIS-u).

njihovih podataka u sustav te registracijski broj prijevoznog sredstva⁹⁰⁹. Te se informacije mogu upotrebljavati samo u svrhe opažanja, izvješćivanja ili izvršavanja određenih inspekcija ili u svrhe strateške ili operativne analize u vezi s osobama osumnjičenima za kršenje carinskih propisa.

Pristup CIS-u dopušten je nacionalnim carinskim, poreznim, poljoprivrednim, javnozdravstvenim i policijskim tijelima, kao i Europolu i Eurojustu.

Obrada osobnih podataka mora biti u skladu s posebnim pravilima utvrđenima Uredbom (EZ) br. 515/97 i Odlukom Vijeća 2009/917/PUP, kao i odredbama Opće uredbe o zaštiti podataka, Uredbe o zaštiti podataka u institucijama Europske unije, modernizirane Konvencije br. 108 i Preporuke o policiji. EDPS je odgovoran za nadzor sukladnosti CIS-a s Uredbom (EZ) br. 45/2001. Sastaje se barem jednom godišnje sa svim nacionalnim tijelima za zaštitu podataka koja su nadležna za nadzor u vezi s CIS-om.

Interoperabilnost informacijskih sustava Europske unije

Upravljanje migracijama, integrirano upravljanje vanjskim granicama EU-a te borba protiv terorizma i prekograničnog kriminala važni su i sve složeniji izazovi u današnjem globaliziranom svijetu. U posljednjih nekoliko godina EU razvija novi sveobuhvatan pristup zaštiti i očuvanju sigurnosti bez dovođenja u pitanje vrijednosti i temeljnih sloboda EU-a. U tim je nastojanjima ključna učinkovita razmjena informacija među nacionalnim tijelima za izvršavanje zakonodavstva te među državama članicama i nadležnim agencijama EU-a⁹¹⁰. Postojeći informacijski sustavi EU-a za upravljanje granicama i unutarnju sigurnost imaju vlastite ciljeve, institucijsku organizaciju, ispitanike i korisnike. EU radi na otklanjanju nedostataka rascjepkanog upravljanja podacima u EU-u među različitim informacijskim sustavima kao što su SIS II,

909 Vidjeti Odluku o CIS-u, članci 24., 25. i 28.

910 Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu i Vijeću: Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. travnja 2016., Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu, Europskom vijeću i Vijeću: Povećanje sigurnosti u svijetu mobilnosti: bolja razmjena informacija u borbi protiv terorizma i jače vanjske granice, COM(2016) 602 final, Bruxelles, 14. rujna 2016., Europska komisija (2016.), Prijedlog uredbe Europskog parlamenta i Vijeća o upotrebi Schengenskog informacijskog sustava za vraćanje državljana trećih zemalja s nezakonitim boravkom. Vidjeti i Komunikaciju Komisije Europskom parlamentu, Europskom vijeću i Vijeću: Sedmo izvješće o napretku prema uspostavi učinkovite i istinske sigurnosne unije, COM(2017) 261 final, Bruxelles, 16. svibnja 2017.

VIS i Eurodac tako što istražuje mogućnost njihove interoperabilnosti⁹¹¹. Glavni je cilj osigurati da nadležna policijska, carinska i pravosudna tijela sustavno primaju informacije koje su im potrebne za izvršavanje dužnosti te istovremeno održati ravnotežu u pogledu prava na privatnost, zaštitu podataka i druga temeljna prava.

Interoperabilnost je „sposobnost informacijskih sustava da razmjenjuju podatke i omogućuju dijeljenja informacija”⁹¹². Tom se razmjenom ne smiju ugroziti nužna stroga pravila o pristupu i upotrebi koja su zajamčena Općom uredbom o zaštiti podataka, Direktivom o zaštiti podataka za policiju i tijela kaznenog pravosuđa i Poveljom EU-a o temeljnim pravima te svi ostali relevantni propisi. Integrirana rješenja za upravljanje podacima ne smiju utjecati na načela ograničenja svrhe ili tehničke ili integrirane zaštite podataka⁹¹³.

Uz poboljšanje funkcija triju glavnih informacijskih sustava – sustava SIS II, VIS i Eurodac – Komisija je predložila uspostavu četvrtog centraliziranog sustava za upravljanje granicama koji bi obuhvaćao državljane trećih zemalja: sustav ulaska/izlaska (EES)⁹¹⁴, čije se uvođenje planira za 2020.⁹¹⁵ Komisija je također izdala prijedlog o uspostavi Europskog sustava za informacije o putovanjima i njihovu odobrenju (ETIAS)⁹¹⁶, u kojemu će se prikupljati informacije o osobama koje putuju bez vize u EU kako bi se omogućile napredne provjere u vezi s nezakonitim migracijama i sigurnosne provjere.

911 Vijeće Europske unije (2005.), Haški program: jačanje slobode, sigurnosti i pravde u Europskoj uniji, SL 2005 C 53, Europska komisija (2010.), Komunikacija Komisije Europskom parlamentu i Vijeću: Pregled upravljanja informacijama u području slobode, sigurnosti i pravde, COM(2010) 385 final, Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu i Vijeću: Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. travnja 2016., Europska komisija (2016.), Odluka Komisije od 17. lipnja 2016. o osnivanju skupine stručnjaka na visokoj razini za informacijske sustave i interoperabilnost, SL 2016 C 257.

912 Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu i Vijeću: Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. travnja 2016., str. 14.

913 *Ibid.*, str. 4.–5.

914 Europska komisija (2016.), Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi sustava ulaska/izlaska (EES) za registraciju podataka o ulasku i izlasku te podataka o zabrani ulaska za državljane trećih zemalja koji prelaze vanjske granice država članica Europske unije i određivanju uvjeta za pristup EES-u za potrebe kaznenog progona te o izmjeni Uredbe (EZ) br. 767/2008 i Uredbe (EZ) br. 1077/2011, COM(2016) 194 final, Bruxelles, 6. travnja 2016.

915 Europska komisija (2016.), Komunikacija Komisije Europskom parlamentu i Vijeću: Jači i pametniji informacijski sustavi za granice i sigurnost, COM(2016) 205 final, Bruxelles, 6. travnja 2016., str. 5.

916 Europska komisija (2016.), Prijedlog uredbe Europskog parlamenta i Vijeća o uspostavi europskog sustava za informacije o putovanjima i njihovu odobrenju (ETIAS) i izmjeni uredbi (EU) br. 515/2014, (EU) 2016/399, (EU) 2016/794 i (EU) 2016/1624, COM(2016) 731 final, 16. studenoga 2016.

9

Posebne vrste podataka i s njima povezani propisi o zaštiti podataka

EU	Obuhvaćena pitanja	Vijeće Europe
Opća uredba o zaštiti podataka Direktiva o privatnosti i elektroničkim komunikacijama	Elektroničke komunikacije	Modernizirana Konvencija br. 108 Preporuka o telekomunikacijskim uslugama
Opća uredba o zaštiti podataka, članak 88.	Radni odnosi	Modernizirana Konvencija br. 108 Preporuka o zaposlenju <i>ESLJP, Copland protiv Ujedinjene Kraljevine</i> , br. 62617/00, 2007.
Opća uredba o zaštiti podataka, članak 9. stavak 2. točke (h) i (i)	Medicinski podaci	Modernizirana Konvencija br. 108 Preporuka o medicinskim podacima <i>ESLJP, Z protiv Finske</i> , br. 22009/93, 1997.
Uredba o kliničkim ispitivanjima	Klinička ispitivanja	
Opća uredba o zaštiti podataka, članak 6. stavak 4. i članak 88.	Statistika	Modernizirana Konvencija br. 108 Preporuka o statističkim podacima
Uredba (EZ) br. 223/2009 o europskoj statistici <i>SEU, C-524/06, Huber protiv Bundesrepublik Deutschland [VV]</i> , 2008.	Službena statistika	Modernizirana Konvencija br. 108 Preporuka o statističkim podacima

EU	Obuhvaćena pitanja	Vijeće Europe
Direktiva 2014/65/EU o tržištu financijskih instrumenata Uredba (EU) br. 648/2012 o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju Uredba (EZ) br. 1060/2009 o agencijama za kreditni rejting Direktiva 2007/64/EZ o platnim uslugama na unutarnjem tržištu	Financijski podaci	Modernizirana Konvencija br. 108 Preporuka 90 (19) koja se upotrebljava za plaćanja i druge srodne aktivnosti ESLJP, <i>Michaud protiv Francuske</i>, br. 12323/11, 2012.

U nekoliko su slučajeva na europskoj razini doneseni posebni pravni instrumenti kojima se u određenim situacijama detaljnije primjenjuju opća pravila modernizirane Konvencije br. 108 ili Opće uredbe o zaštiti podataka.

9.1. Elektroničke komunikacije

Ključne točke

- Posebna pravila o zaštiti podataka u području telekomunikacija, s posebnim naglaskom na telefonske usluge, sadržana su u Preporuci Vijeća Europe iz 1995.
- Obrada osobnih podataka koji se odnose na pružanje komunikacijskih usluga na razini Europske unije uređena je Direktivom o privatnosti i elektroničkim komunikacijama.
- Povjerljivost elektroničkih komunikacija odnosi se ne samo na sadržaj komunikacije već i na metapodatke, kao što su informacije o tome tko je komunicirao s kime, kad se komunikacija odvijala i koliko je dugo trajala, kao i na podatke o lokaciji, kao što je lokacija s koje su podaci priopćeni.

U komunikacijskim je mrežama veća mogućnost neopravdanog miješanja u osobnu sferu korisnika zbog razvijenih tehničkih mogućnosti prisluškivanja i praćenja komunikacije koja se odvija putem takvih mreža. Zbog toga se smatralo da su potrebni posebni propisi o zaštiti podataka radi otklanjanja određenih rizika kojima su izloženi korisnici komunikacijskih usluga.

Vijeće Europe izdalo je 1995. godine Preporuku o zaštiti podataka u području telekomunikacija koja se naročito odnosila na telefonske usluge⁹¹⁷. Sukladno toj preporuci, svrhe prikupljanja i obrade osobnih podataka u kontekstu telekomunikacija treba ograničiti na: spajanje korisnika na mrežu, ponudu određene telekomunikacijske usluge, naplatu, provjeru, osiguravanje optimalnog tehničkog rada i razvoj mreže i usluge.

Posebna je pažnja posvećena i uporabi komunikacijskih mreža za slanje poruka direktnog marketinga. Poruke direktnog marketinga u pravilu ne smiju biti usmjerene pretplatniku koji je izričito izjavio da ih ne želi primati. Uređaji za automatsko pozivanje koji prenose unaprijed snimljene promidžbene poruke smiju se upotrebljavati samo ako je pretplatnik dao svoju izričitu privolu. Nacionalnim zakonodavstvom propisuju se detaljna pravila u tom području.

U sklopu **pravnog okvira EU-a**, nakon prvog pokušaja 1997., Direktiva o privatnosti i elektroničkim komunikacijama donesena je 2002. i izmijenjena 2009. To je učinjeno radi nadopunjavanja i prilagođavanja odredaba nekadašnje Direktive o zaštiti podataka telekomunikacijskom sektoru⁹¹⁸.

Primjena Direktive o privatnosti i elektroničkim komunikacijama ograničena je na komunikacijske usluge u javnim elektroničkim mrežama.

U Direktivi o privatnosti i elektroničkim komunikacijama razlikuju se tri glavne kategorije podataka nastalih pri komuniciranju:

- podaci koji čine sadržaj poruka poslanih tijekom komuniciranja – ti su podaci strogo povjerljivi,

917 Vijeće Europe, Odbor ministara (1995.), Preporuka Rec(95)4 državama članicama o zaštiti osobnih podataka u području telekomunikacijskih usluga, s posebnim naglaskom na telefonske usluge, 7. veljače 1995.

918 Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija, SL 2002 L 201 (Direktiva o privatnosti i elektroničkim komunikacijama), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge, Direktive 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredbe (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača, SL 2009 L 337.

- podaci potrebni za uspostavu i održavanje komunikacije, takozvani metapodaci, koji se u Direktivi nazivaju „podaci o prometu“, kao što su informacije o osobama koje komuniciraju, vremenu i trajanju komunikacije,
- metapodaci obuhvaćaju podatke koji se posebno odnose na lokaciju komunikacijskog uređaja, takozvane podatke o lokaciji – ti su podaci istovremeno podaci o lokaciji korisnika komunikacijskih uređaja, posebno kad je riječ o korisnicima mobilnih komunikacijskih uređaja.

Podatke o prometu može upotrebljavati pružatelj usluge za potrebe naplate usluge i za tehničko pružanje usluge. Međutim, uz privolu ispitanika, ti se podaci mogu otkriti drugim voditeljima obrade koji pružaju usluge dodane vrijednosti, kao što je pružanje informacija u vezi s lokacijom korisnika, o sljedećem stajalištu podzemne željeznice ili ljekarne ili o vremenskoj prognozi za tu lokaciju.

Prema članku 15. Direktive o privatnosti i elektroničkim komunikacijama, ostali pristupi podacima o komunikacijama u elektroničkim mrežama moraju ispunjavati zahtjeve za opravdano miješanje u pravo na zaštitu podataka kako je utvrđeno u članku 8. stavku 2. EKLJP-a i potvrđeno u člancima 8. i 52. Povelje EU-a o temeljnim pravima. Takav pristup može uključivati pristup u svrhu istraga kaznenih djela.

Izmjenama Direktive o privatnosti i elektroničkim komunikacijama iz 2009.⁹¹⁹ uvedeno je sljedeće:

- Ograničenja za slanje e-pošte u svrhu direktnog marketinga proširena su na usluge kratkih (SMS) poruka, usluge multimedijских poruka i ostale vrste sličnih aplikacija. Promidžbena e-pošta zabranjena je osim uz prethodnu privolu. Bez takve privole dopušteno je obraćanje promidžbenom e-poštom samo prijašnjim kupcima ako su pružili svoje adrese e-pošte i nemaju primjedbi na to.
- Državama članicama nametnuta je obveza pružanja pravnih lijekova protiv kršenja zabrane neželjene komunikacije⁹²⁰.

919 Direktiva 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o izmjeni Direktive 2002/22/EZ o univerzalnim uslugama i pravima korisnika s obzirom na elektroničke komunikacijske mreže i usluge, Direktive 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija i Uredbe (EZ) br. 2006/2004 o suradnji između nacionalnih tijela odgovornih za provedbu zakona o zaštiti potrošača, SL 2009 L 337.

920 Vidjeti izmijenjenu Direktivu, članak 13.

- Postavljanje kolačića, softvera koji nadzire i bilježi aktivnosti korisnika računala, više nije dopušteno bez privole korisnika računala. Nacionalnim zakonodavstvom treba detaljnije urediti kako treba izraziti i pribaviti privolu radi osiguravanja odgovarajuće zaštite⁹²¹.

Ako dođe do povrede podataka zbog neovlaštenog pristupa, gubitka ili uništavanja podataka, o tome je potrebno odmah obavijestiti nadležno nadzorno tijelo. Pretplatnike je potrebno obavijestiti ako je šteta koju su eventualno pretrpjeli posljedica povrede podataka⁹²².

Prema Direktivi o zadržavanju podataka⁹²³, pružatelji komunikacijskih usluga bili su dužni zadržavati metapodatke. Međutim, SEU je tu direktivu proglasio nevaljanom (više pojedinosti potražiti u [dijelu 8.3.](#)).

Izgledi

U siječnju 2017. Europska komisija donijela je novi Prijedlog uredbe o e-privatnosti koja bi zamijenila nekadašnju Direktivu o privatnosti i elektroničkim komunikacijama. Glavni cilj i dalje bi bila zaštita „temeljnih prava i sloboda fizičkih i pravnih osoba pri pružanju i uporabi elektroničkih komunikacijskih usluga, posebno prava na poštovanje privatnog života i komuniciranja i zaštita fizičkih osoba u pogledu obrade osobnih podataka“. Novom Uredbom istodobno bi se osiguralo slobodno kretanje elektroničkih komunikacijskih podataka i elektroničkih komunikacijskih usluga unutar Unije⁹²⁴. Dok se Općom uredbom o zaštiti podataka prvenstveno upućuje na članak 8. Povelje EU-a o temeljnim pravima, predloženom Uredbom nastoji se ugraditi članak 7. Povelje u sekundarno pravo Unije.

Uredbom bi se odredbe prijašnje Direktive prilagodile novim tehnologijama i tržištu te bi se izgradio sveobuhvatan i dosljedan okvir u sklopu Opće uredbe o zaštiti

921 Vidjeti *ibid.*, članak 5.; vidjeti i Radna skupina iz članka 29. (2012.), *Mišljenje 04/2012 o izuzeću od obveze davanja privole za postavljanje kolačića*, WP 194, Bruxelles, 7. lipnja 2012.

922 Vidjeti i Radna skupina iz članka 29. (2011.), *Radni dokument 01/2011 o trenutačnom okviru Europske unije za povredu osobnih podataka i preporukama za budući razvoj politike*, WP 184, Bruxelles, 5. travnja 2011.

923 Direktiva 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ, SL 2006 L 105.

924 Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) (COM(2017) 10 final), članak 1.

podataka. U tom smislu Uredba o e-privatnosti bila bi *lex specialis* za Opću uredbu o zaštiti podataka, kojim bi se ona prilagodila elektroničkim komunikacijskim podacima koji čine osobne podatke. Novom Uredbom obuhvaća se obrada „elektroničkih komunikacijskih podataka“, uključujući sadržaj elektroničkih komunikacija i meta-podatke koji nisu nužno osobni podaci. Njezino područje primjene ograničeno je na EU, uključujući slučajeve u kojima se podaci prikupljeni u EU-u obrađuju izvan EU-a, a proširuje se na pružatelje komunikacijskih usluga OTT (engl. *Over The Top*). To su pružatelji usluga koji isporučuju sadržaj, usluge ili aplikacije putem interneta bez izravnog uključivanja mrežnog operatera ili pružatelja internetskih usluga (ISP). Primjeri takvih pružatelja usluga uključuju Skype (glasovni pozivi i videopozivi), WhatsApp (razmjena poruka), Google (pretraživanje), Spotify (glazba) i Netflix (videosa-držaj). Mehanizmi provedbe Opće uredbe o zaštiti podataka primjenjivali bi se i na novu Uredbu.

Donošenje Uredbe o e-privatnosti predviđeno je prije 25. svibnja 2018., kada Opća uredba o zaštiti podataka stupa na snagu za svih 28 država članica. Međutim, to ovisi o odobrenju i Europskog parlamenta i Vijeća⁹²⁵.

9.2. Podaci o zaposlenju

Ključne točke

- Posebna pravila o zaštiti podataka u okviru radnih odnosa sadržana su u Preporuci o podacima o zaposlenju Vijeća Europe.
- U Općoj uredbi o zaštiti podataka radni odnosi spominju se konkretno samo u kontekstu obrade osjetljivih podataka.
- Valjanost privole, koja mora biti dana dobrovoljno, kao pravne osnove za obradu podataka o zaposlenicima može biti dvojben s obzirom na ekonomsku neravnotežu između poslodavca i zaposlenika. Okolnosti davanja privole moraju se pažljivo procijeniti.

⁹²⁵ Za više informacija vidjeti Europska komisija (2017.), „Komisija predlaže pravila o visokoj razini zaštite privatnosti za sve elektroničke komunikacije te ažurira pravila o zaštiti podataka za institucije EU-a“, priopćenje za medije, 10. siječnja 2017.

Obrada podataka u kontekstu radnih odnosa podliježe općem zakonodavstvu EU-a koje se odnosi na zaštitu osobnih podataka. Međutim, jedna se uredba⁹²⁶ posebno odnosi na zaštitu obrade osobnih podataka u europskim institucijama u kontekstu zapošljavanja (među ostalim). U Općoj uredbi o zaštiti podataka radni odnosi posebno se spominju u članku 9. stavku 2., kojim se utvrđuje da se osobni podaci mogu obrađivati prilikom izvršavanja obveza ili ostvarivanja posebnih prava voditelja obrade ili ispitanika u području zaposlenja.

Prema Općoj uredbi o zaštiti podataka, zaposlenici bi trebali imati mogućnost jasno razlikovati podatke za čiju su obradu/pohranu dali dobrovoljnu privolu i svrhe u koje se njihovi podaci pohranjuju. Zaposlenici također trebaju biti informirani o svojim pravima i razdoblju pohrane podataka prije nego što daju privolu. Ako postoji vjerojatnost da bi povreda osobnih podataka dovela do visokog rizika u pogledu prava i sloboda pojedinaca, poslodavac mora o toj povredi obavijestiti zaposlenika. Članom 88. Uredbe državama članicama dopušta se da utvrde preciznija pravila s ciljem osiguravanja zaštite prava i sloboda zaposlenika u vezi s obradom njihovih osobnih podataka u kontekstu zaposlenja.

Primjer: U predmetu *Worten*⁹²⁷ podaci su uključivali zapis o radnom vremenu koji je sadržavao razdoblja rada i odmora u danu, što predstavlja osobne podatke. Nacionalnim se zakonodavstvom poslodavca može obvezati da zapise o radnom vremenu stavi na raspolaganje nacionalnim tijelima nadležnim za nadzor uvjeta rada. Time bi se omogućio izravan pristup odgovarajućim osobnim podacima. Međutim, pristup osobnim podacima nužan je kako bi se nacionalnom tijelu omogućio nadzor zakonodavstva o uvjetima rada⁹²⁸.

Što se tiče **Vijeća Europe**, Preporuka o podacima o zaposlenju izdana je 1989. i revidirana 2015.⁹²⁹ Preporuka obuhvaća obradu osobnih podataka u svrhe zapošljavanja u privatnom i javnom sektoru. Obrada mora biti u skladu s određenim načelima i ograničenjima, poput načela transparentnosti i savjetovanja s predstavnicima

926 Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka, SL 2001 L 8.

927 SEU, C-342/12, *Worten – Equipamentos para o Lar, SA protiv Autoridade para as Condições de Trabalho (ACT)*, 30. svibnja 2013., t. 19.

928 *Ibid.*, t. 43.

929 Vijeće Europe, Odbor ministara (2015.), Preporuka Rec(2015)5 državama članicama o obradi osobnih podataka u kontekstu zapošljavanja, travanj 2015.

zaposlenika prije uvođenja nadzornih sustava na radnom mjestu. U Preporuci se također navodi da poslodavci trebaju primjenjivati preventivne mjere, poput filtara, umjesto nadziranja upotrebe interneta zaposlenika.

Pregled najčešćih problema u vezi sa zaštitom podataka u kontekstu zapošljavanja nalazi se u radnom dokumentu Radne skupine iz članka 29.⁹³⁰ Radna skupina analizirala je važnost privole kao pravne osnove za obradu podataka o zaposlenosti⁹³¹. Utvrdila je da će zbog ekonomske neravnoteže između poslodavca koji traži privolu i zaposlenika koji daje privolu uvijek biti dvojbeno je li privola dana dobrovoljno. Stoga pri procjeni valjanosti privole u kontekstu zapošljavanja valja pažljivo razmotriti okolnosti u kojima se privola upotrebljava kao pravna osnova za obradu podataka.

Čest problem u vezi sa zaštitom podataka u današnjem tipičnom radnom okruženju jest opseg legitimnog nadzora elektroničkih komunikacija zaposlenika na radnom mjestu. Često se tvrdi da se taj problem može lako riješiti zabranom privatne uporabe komunikacijskih sredstava na radnom mjestu. Međutim, takva bi opća zabrana mogla biti nerazmjerna i nerealna. Presude ESLJP-a u predmetima *Copland protiv Ujedinjene Kraljevine* i *Bărbulescu protiv Rumunjske* posebno su važne u tom kontekstu.

Primjer: U predmetu *Copland protiv Ujedinjene Kraljevine*⁹³² tajno je nadzirana uporaba telefona, e-pošte i interneta zaposlenice više škole kako bi se utvrdilo upotrebljava li prekomjerno školska sredstva u osobne svrhe. ESLJP je smatrao da su telefonski pozivi iz poslovnih prostorija obuhvaćeni pojmovima privatnog života i dopisivanja. Stoga su takvi pozivi i e-pošta upućeni s radnog mjesta, kao i informacije dobivene na temelju nadzora osobne uporabe interneta, zaštićeni člankom 8. EKLJP-a. U slučaju tužiteljice nisu postojale odredbe kojima se uređuju okolnosti u kojima poslodavci mogu nadzirati zaposlenikovu uporabu telefona, e-pošte i interneta. Stoga miješanje nije bilo u skladu sa zakonom. ESLJP je stoga zaključio da je došlo do kršenja članka 8. Konvencije.

930 Radna skupina iz članka 29. (2017.), *Mišljenje 2/2017 o obradi podataka na radnom mjestu*, WP 249, Bruxelles, 8. lipnja 2017.

931 Radna skupina iz članka 29. (2005.), *Radni dokument o zajedničkom tumačenju članka 26. stavka 1. Direktive 95/46/EZ od 24. listopada 1995.*, WP 114, Bruxelles, 25. studenoga 2005.

932 ESLJP, *Copland protiv Ujedinjene Kraljevine*, br. 62617/00, 3. travnja 2007.

Primjer: U predmetu *Bărbulescu protiv Rumunjske*⁹³³ tužitelj je otpušten zbog upotrebe interneta tijekom radnog vremena, čime je prekršio interna pravila. Njegov je poslodavac nadzirao njegove komunikacije. Zapisi u kojima su vidljive poruke posve osobne naravi predloženi su u sklopu postupka u njihovoj državi. ESLJP je utvrdio da je članak 8. primjenjiv u ovom slučaju i ostavio je otvorenim pitanje je li na temelju ograničavajućih pravila poslodavca tužitelj mogao razumno očekivati privatnost, no zaključio je da poslodavac svojim naporima ne može posve onemogućiti privatni društveni život na radnom mjestu.

Kad je riječ o osnovanosti takva postupka, državama ugovornim strankama trebalo je omogućiti velik raspon procjena prilikom ocjenjivanja potrebe za uspostavljanjem pravnog okvira kojim se reguliraju uvjeti u kojima poslodavac može kontrolirati elektroničke i druge neposlovne komunikacije zaposlenika na radnom mjestu. Unatoč tome, nacionalna tijela morala su osigurati da je poslodavčevo uvođenje mjera za nadziranje dopisivanja i drugih komunikacija, neovisno o opsegu i trajanju takvih mjera, popraćeno odgovarajućim i dostatnim zaštitnim mjerama protiv zlouporabe. Proporcionalnost i postupovna jamstva protiv proizvoljnog postupanja bili su od ključne važnosti, a ESLJP je utvrdio niz čimbenika koji su bili relevantni u tim okolnostima. Takvi su čimbenici, među ostalim, uključivali mjeru u kojoj poslodavac nadzire zaposlenike, razinu miješanja u privatnost zaposlenika, posljedice za zaposlenika i postojanje odgovarajućih zaštitnih mjera. Usto, nacionalna tijela morala su osigurati da zaposlenik čije se komunikacije nadziru ima pristup pravnom lijeku pred pravosudnim tijelom s nadležnošću da utvrdi, barem u suštini, kako se ti navedeni kriteriji poštuju i jesu li sporne mjere zakonite.

U ovom slučaju ESLJP je utvrdio da je došlo do kršenja članka 8. jer nacionalna tijela nisu omogućila odgovarajuću zaštitu prava tužitelja na poštovanje njegova privatnog života i dopisivanje te stoga nisu uspostavila pravednu ravnotežu između predmetnih interesa.

Prema preporuci Vijeća Europe o zaposlenju, osobne podatke koji se prikupljaju u svrhu zaposlenja treba dobiti izravno od pojedinog zaposlenika.

933 ESLJP, *Bărbulescu protiv Rumunjske* [VV], br. 61496/08, 5. rujna 2017., t. 121.

Osobni podaci koji se prikupljaju radi zapošljavanja moraju se ograničiti na informacije koje su potrebne za procjenu prikladnosti kandidata i njihova radnog potencijala.

U Preporuci se također posebno spominju podaci o mišljenju o učinkovitosti ili potencijalu pojedinih zaposlenika. Podaci o mišljenju moraju se temeljiti na poštenim i pravednim ocjenama i ne smiju biti uvredljivo formulirani. To je uvjetovano načelima poštene obrade podataka i točnosti podataka.

Poseban je vid zakonodavstva o zaštiti podataka u odnosu između zaposlenika i poslodavca uloga predstavnika zaposlenika. Predstavnici smiju primati osobne podatke o zaposlenicima samo ako je to nužno da bi mogli zastupati interese zaposlenika ili ako su takvi podaci nužni za ispunjavanje ili nadzor obveza utvrđenih kolektivnim ugovorima.

Osjetljivi osobni podaci koji se prikupljaju u svrhe zaposlenja smiju se obrađivati samo u određenim slučajevima i u skladu sa zaštitnim mjerama koje se propisuju nacionalnim zakonodavstvom. Poslodavci mogu zaposlenike ili kandidate za posao pitati o njihovom zdravstvenom stanju ili ih podvrgnuti zdravstvenom pregledu samo ako je to nužno. Razlozi za to mogu biti: utvrđivanje njihove prikladnosti za radno mjesto, ispunjavanje zahtjeva preventivne medicine, zaštita vitalnih interesa ispitanika ili drugih zaposlenika i pojedinaca, omogućivanje dodjele socijalnih davanja ili odgovaranje na sudske zahtjeve. Zdravstveni podaci smiju se prikupljati samo od dotičnog zaposlenika, a ne iz drugih izvora, osim uz izričitu privolu i privolu utemeljenu na informacijama ili ako je to propisano nacionalnim zakonodavstvom.

U skladu s Preporukom o zaposlenju, zaposlenici trebaju biti informirani o svrsi obrade njihovih osobnih podataka, vrsti prikupljenih osobnih podataka, tijelima kojima se podaci redovito priopćuju te svrsi i pravnoj osnovi takvih priopćenja. Elektroničkim komunikacijama na radnom mjestu može se pristupiti samo u svrhu sigurnosti ili drugih legitimnih razloga, a takav je pristup dozvoljen tek nakon što zaposlenici budu obaviješteni da poslodavac može pristupiti takvim komunikacijama.

Zaposlenici moraju imati pravo na pristup svojim podacima o zaposlenju, kao i pravo na njihov ispravak ili brisanje. Ako se obrađuju podaci o mišljenju, zaposlenici moraju imati pravo osporiti mišljenje. Međutim, ta prava mogu biti privremeno ograničena u svrhu unutarnjih istraga. Ako se zaposleniku uskrati pristup, ispravak ili brisanje osobnih podataka o zaposlenju, nacionalnim zakonodavstvom moraju se propisati odgovarajući postupci kojima se osporava takvo uskraćivanje.

9.3. Zdravstveni podaci

Ključna točka

- Medicinski su podaci osjetljivi, stoga uživaju posebnu zaštitu.

Osobni podaci u vezi sa zdravljem ispitanika smatraju se posebnom kategorijom podataka sukladno članku 9. stavku 1. Opće uredbe o zaštiti podataka i članku 6. modernizirane Konvencije br. 108. Stoga podaci povezani sa zdravljem podliježu strožem režimu obrade podataka od neosjetljivih podataka. Općom uredbom o zaštiti podataka zabranjuje se obrada „osobnih podataka koji se odnose na zdravlje” (koji podrazumijevaju „sve podatke koji se odnose na zdravstveno stanje ispitanika, a koji otkrivaju informacije u vezi s prijašnjim, trenutačnim ili budućim fizičkim ili mentalnim zdravstvenim stanjem ispitanika”)⁹³⁴ te genetičkih i biometrijskih podataka, osim ako je to dozvoljeno člankom 9. stavkom 2. Obje su te vrste podataka dodane na popis „posebnih kategorija podataka”⁹³⁵.

Primjer: U predmetu *Z protiv Finske*⁹³⁶ bivši suprug tužiteljice, koji je bio zaražen HIV-om, počinio je niz spolnih kaznenih djela. Kasnije je osuđen za ubojstvo iz nehaja jer je svoje žrtve svjesno izložio riziku od zaraze HIV-om. Nacionalni je sud naložio da cjelokupna presuda i dokumenti iz predmeta ostanu povjerljivi 10 godina unatoč zahtjevima tužiteljice za produljenje razdoblja povjerljivosti. Žalbeni sud odbio je te zahtjeve, a presuda je sadržavala imena i prezimena i tužiteljice i njezina bivšeg supruga. ESLJP je smatrao da miješanje nije bilo nužno u demokratskom društvu jer je zaštita medicinskih podataka od temeljne važnosti za ostvarenje prava na poštovanje privatnog i obiteljskog života, a naročito kad se radi o informacijama o zarazi HIV-om jer je ta bolest stigmatizirana u mnogim društvima. Stoga je ESLJP zaključio da bi se odobravanjem pristupa presudi žalbenog suda u kojoj se navode identitet i zdravstveno stanje tužiteljice po isteku razdoblja od 10 godina nakon donošenja presude prekršio članak 8. EKLJP-a.

⁹³⁴ Opća uredba o zaštiti podataka, uvodna izjava 35.

⁹³⁵ *Ibid.*, članak 2.

⁹³⁶ ESLJP, *Z protiv Finske*, br. 22009/93, 25. veljače 1997., t. 94. i 112.; vidjeti i ESLJP, *M. S. protiv Švedske*, br. 20837/92, 27. kolovoza 1997.; ESLJP, *L. L. protiv Francuske*, br. 7508/02, 10. listopada 2006.; ESLJP, *I. protiv Finske*, br. 20511/03, 17. srpnja 2008.; ESLJP, *K. H. i drugi protiv Slovačke*, br. 32881/04, 28. travnja 2009.; ESLJP, *Szuluk protiv Ujedinjene Kraljevine*, br. 36936/05, 2. lipnja 2009.

U okviru **prava EU-a**, člankom 9. stavkom 2. točkom (h) Opće uredbe o zaštiti podataka omogućuje se obrada medicinskih podataka kada je ona nužna radi preventivne medicine, medicinske dijagnoze, pružanja zdravstvene skrbi ili tretmana ili u svrhu upravljanja zdravstvenim uslugama. Međutim, obrada je dopuštena samo ako je provodi zdravstveni radnik koji ima obvezu čuvanja poslovne tajne ili druga osoba koja ima istu obvezu.

U okviru **prava Vijeća Europe**, u Preporuci Vijeća Europe o medicinskim podacima iz 1997. na obradu podataka u području medicine detaljnije se primjenjuju načela Konvencije br. 108⁹³⁷. Predložena su pravila u skladu s onima iz Opće uredbe o zaštiti podataka u pogledu zakonitih svrha obrade medicinskih podataka, obveza čuvanja poslovne tajne osoba koje upotrebljavaju zdravstvene podatke te prava ispitanika na transparentnost i pristup, ispravak i brisanje. Osim toga, medicinski podaci koje zdravstveni radnici zakonito obrađuju ne smiju se prenositi tijelima za izvršavanje zakonodavstva ako nisu osigurane „odgovarajuće zaštitne mjere kojima se sprečava otkrivanje koje nije u skladu s pravom na poštovanje [...] privatnog života koje je zajamčeno člankom 8. Europske konvencije o ljudskim pravima”⁹³⁸. Nacionalno zakonodavstvo također mora biti „formulirano dovoljno precizno i osiguravati odgovarajuću pravnu zaštitu od proizvoljnosti”⁹³⁹.

Osim toga, Preporuka o medicinskim podacima sadržava posebne odredbe o medicinskim podacima nerođene djece i nemoćnih osoba, kao i o obradi genetskih podataka. Znanstvena istraživanja izričito su priznata kao razlog za čuvanje podataka dulje nego što su potrebni, iako to najčešće zahtijeva anonimizaciju. U članku 12. Preporuke o medicinskim podacima predlažu se detaljni propisi za situacije u kojima su istraživačima potrebni osobni podaci, a anonimizirani podaci nisu dovoljni.

Pseudonimizacija može biti dobar način za ispunjavanje znanstvenih potreba i zaštitu interesa pacijenata. Koncept pseudonimizacije u kontekstu zaštite podataka detaljnije je pojašnjen u [dijelu 2.1.1](#).

937 Vijeće Europe, Odbor ministara (1997.), Preporuka Rec(97)5 državama članicama o zaštiti medicinskih podataka, 13. veljače 1997. Napominjemo da je u tijeku revizija te preporuke.

938 ESLJP, *Avilkina i drugi protiv Rusije*, br. 1585/09, 6. lipnja 2013., t. 53. Vidjeti i ESLJP, *Biriuk protiv Litve*, br. 23373/03, 25 studenoga 2008.

939 ESLJP, *L. H. protiv Latvije*, br. 52019/07, 29. travnja 2014., t. 59.

Preporuka Vijeća Europe iz 2016. o podacima koji proizlaze iz genetičkih ispitivanja primjenjuje se i na obradu podataka u području medicine⁹⁴⁰. Preporuka je izuzetno važna za e-zdravstvo, u sklopu kojeg se informacijsko-komunikacijske tehnologije (IKT) upotrebljavaju za lakše pružanje zdravstvene skrbi. Primjer je slanje rezultata testa očinstva nekog pacijenta od jednog pružatelja zdravstvenih usluga drugome. Cilj je Preporuke zaštititi prava osoba čiji se osobni podaci obrađuju u svrhe osiguranja protiv rizika u vezi sa zdravljem, tjelesnim integritetom, dobi ili smrti osobe. Društva za osiguranje moraju opravdati obradu zdravstvenih podataka i ona mora biti proporcionalna prirodi i važnosti rizika koji se razmatra. Obrada ove vrste podataka ovisi o privoli ispitanika. Društva za osiguranje trebaju uspostaviti i zaštitne mjere za pohranu zdravstvenih podataka.

Klinička ispitivanja, koja uključuju ocjenjivanje učinaka novih lijekova na bolesnike u okruženjima dokumentiranih ispitivanja, imaju znatne implikacije na zaštitu podataka. Klinička ispitivanja lijekova koji služe ljudskoj uporabi reguliraju se Uredbom (EU) br. 536/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o kliničkim ispitivanjima lijekova za primjenu kod ljudi te o stavljanju izvan snage Direktive 2001/20/EZ (Uredba o kliničkim ispitivanjima)⁹⁴¹. Glavni su elementi Uredbe o kliničkim ispitivanjima sljedeći:

- pojednostavljen postupak prijave putem portala EU-a⁹⁴²,
- rokovi za ocjenu zahtjeva za klinička ispitivanja⁹⁴³,
- sudjelovanje etičkog odbora u postupku ocjenjivanja u skladu sa zakonima država članica (i europskim pravom kojim se utvrđuju predmetni rokovi)⁹⁴⁴, te
- poboljšana transparentnost kliničkih ispitivanja i njihovih ishoda⁹⁴⁵.

940 Vijeće Europe, Odbor ministara (2016.), Preporuka Rec(2016)8 državama članicama o obradi osobnih zdravstvenih podataka u svrhu osiguranja, uključujući podatke iz genetičkih ispitivanja, 26. listopada 2016.

941 Uredba (EU) br. 536/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o kliničkim ispitivanjima lijekova za primjenu kod ljudi te o stavljanju izvan snage Direktive 2001/20/EZ (Uredba o kliničkim ispitivanjima), SL 2014 L 158.

942 Uredba o kliničkim ispitivanjima, članak 5. stavak 1.

943 *Ibid.*, članak 5. stavci od 2. do 5.

944 *Ibid.*, članak 2. stavak 2. točka 11.

945 *Ibid.*, članak 9. stavak 1. i uvodna izjava 67.

U Općoj uredbi o zaštiti podataka utvrđuje se da se u svrhe pristanka na sudjelovanje u aktivnostima znanstvenog istraživanja u sklopu kliničkih ispitivanja primjenjuje Uredba (EU) br. 536/2014⁹⁴⁶.

U tijeku su i mnoge druge zakonodavne i ostale inicijative EU-a u vezi s osobnim podacima u zdravstvenom sektoru⁹⁴⁷.

Elektronički zdravstveni zapisi

Elektronički zdravstveni zapisi definiraju se kao „sveobuhvatan zdravstveni zapis ili slična dokumentacija o prošlom ili trenutačnom tjelesnom i duševnom stanju pojedinca u elektroničkom obliku, koji omogućuju dostupnost tih podataka radi medicinskog liječenja i drugih usko povezanih svrha”⁹⁴⁸. Elektronički zdravstveni zapisi elektroničke su verzije povijesti bolesti bolesnika i mogu uključivati kliničke podatke koji se odnose na te pojedince, kao što su povijest bolesti, poteškoće i bolesti, lijekovi i terapije te rezultati pregleda i laboratorijski nalazi i izvješća. Tim elektroničkim datotekama, koje mogu sadržavati čitave zapise ili samo izvode ili sažetke, može pristupiti liječnik opće prakse, ljekarnik te drugi zdravstveni radnici. Koncept „e-zdravstva” također se djelomično dotiče zdravstvenih zapisa.

Primjer: Osoba A ugovorila je policu osiguranja s osiguravajućim društvom B. Društvo će prikupljati određene zdravstvene podatke od osobe A, poput trenutačnih zdravstvenih problema ili bolesti. Društvo za osiguranje treba pohranjivati osobne zdravstvene podatke osobe A odvojeno od drugih podataka. Društvo za osiguranje treba pohranjivati i osobne zdravstvene podatke odvojeno od drugih osobnih podataka. To znači da će samo osoba zadužena za predmet osobe A imati pristup njezinim zdravstvenim podacima.

Unatoč tome, elektroničke zdravstvene datoteke dovode do određenih pitanja zaštite podataka, poput njihove dostupnosti, pravilne pohrane i pristupa ispitanika.

Uz elektroničke zdravstvene zapise, 10. travnja 2014. Europska komisija objavila je Zelenu knjigu o mobilnom zdravstvu („m-zdravstvu”) s obzirom na to da je

946 Opća uredba o zaštiti podataka, uvodne izjave 156. i 161.

947 EDPS (2013.), *Mišljenje Europskog nadzornika za zaštitu podataka o priopćenju Komisije o „Akcijском planu za e-zdravlje 2012.–2020.: inovativno zdravstvo za 21. stoljeće”*, Bruxelles, 27. ožujka 2013.

948 Preporuka Komisije od 2. srpnja 2008. o prekograničnoj interoperabilnosti sustava elektroničkih zdravstvenih zapisa (dostupna na engleskom jeziku), točka 3. (c).

m-zdravstvo nov, brzorastući sektor koji ima potencijal transformirati zdravstvo i povećati njegovu učinkovitost i kvalitetu. Taj pojam obuhvaća medicinsku i javnozdravstvenu praksu podržanu putem mobilnih uređaja kao što su mobilni telefoni, uređaji za praćenje bolesnika, osobni digitalni pomoćnici i drugi bežični uređaji te aplikacija (primjerice, aplikacija za zdravlje) koje se mogu povezati s medicinskim uređajima ili senzorima⁹⁴⁹. U knjizi se navode rizici za pravo na zaštitu osobnih podataka koje razvoj m-zdravstva može donijeti te se preporučuje da, s obzirom na osjetljivu prirodu zdravstvenih podataka, njegov razvoj uključuje posebne i primjerene sigurnosne i zaštitne mjere za podatke bolesnika, kao što je šifriranje, te odgovarajuće mehanizme provjere autentičnosti bolesnika kako bi se umanjili sigurnosni rizici. Usklađenost s propisima o zaštiti osobnih podataka, uključujući obvezu pružanja informacija ispitaniku, sigurnost podataka i načelo zakonite obrade osobnih podataka, ključna je za izgradnju povjerenja u rješenja m-zdravstva⁹⁵⁰. U tu svrhu stručnjaci su izradili Kodeks ponašanja na temelju doprinosa širokog raspona dionika, koji uključuju predstavnike sa stručnim iskustvom u zaštiti podataka, samostalnoj i zajedničkoj regulaciji, IKT-u i zdravstvu⁹⁵¹. U vrijeme izrade ovog priručnika nacrt Kodeksa ponašanja podnesen je Radnoj skupini za zaštitu podataka iz članka 29. radi dodavanja napomena i njezina službenog odobrenja.

9.4. Obrada podataka u istraživačke i statističke svrhe

Ključne točke

- Podaci koji se prikupljaju u statističke svrhe ili u svrhe znanstvenog ili povijesnog istraživanja ne smiju se upotrebljavati ni u koju drugu svrhu.
- Podaci koji se zakonito prikupljaju u bilo koju svrhu mogu se dalje upotrebljavati u statističke svrhe ili u svrhe znanstvenog ili povijesnog istraživanja pod uvjetom da su uspostavljene odgovarajuće zaštitne mjere. Anonimizacija ili pseudonimizacija prije prijenosa podataka trećim osobama može pružiti te zaštitne mjere.

949 Europska komisija (2014.), Zelena knjiga o mobilnom zdravstvu („m-zdravstvu“), COM(2014) 219 final, Bruxelles, 10. travnja 2014.

950 *Ibid.*, str. 8.

951 *Draft Code of Conduct on privacy for mobile health applications* (Nacrt kodeksa ponašanja o privatnosti za mobilne aplikacije za zdravlje), 7. lipnja 2016.

Pravom EU-a omogućuje se obrada podataka u statističke svrhe ili u svrhe znanstvenog ili povijesnog istraživanja pod uvjetom da su uspostavljene odgovarajuće zaštitne mjere za prava i slobode ispitanika. One mogu uključivati pseudonimizaciju⁹⁵². Pravom EU-a ili pojedinih država mogu se odrediti određena odstupanja od prava ispitanika ako bi ta prava vjerojatno onemogućila ili ozbiljno ugrozila postizanje legitimne svrhe istraživanja⁹⁵³. Mogu se uvesti odstupanja od ispitanikova prava na pristup, prava na ispravak, prava na ograničenje obrade i prava na prigovor.

Iako podatke koje zakonito prikupi u bilo koju svrhu voditelj obrade može ponovno iskoristiti u vlastite statističke svrhe ili svrhe znanstvenog ili povijesnog istraživanja, podatke treba anonimizirati ili podvrgnuti postupcima kao što je pseudonimizacija, ovisno o kontekstu, prije njihova prenošenja trećoj osobi u statističke svrhe ili svrhe znanstvenog ili povijesnog istraživanja, osim ako je ispitanik za to dao svoju privolu ili ako je to posebno propisano nacionalnim zakonodavstvom. Za razliku od anonimnih podataka, podaci podvrgnuti pseudonimizaciji i dalje podliježu Općoj uredbi o zaštiti podataka⁹⁵⁴.

Uredbom se tako istraživanju dodjeljuje poseban tretman u pogledu općih propisa za zaštitu podataka kako bi se izbjegla ograničenja razvoja istraživanja i postigla sukladnost s ciljem uspostave europskog istraživačkog prostora iz članka 179. UFEU-a. Njome se pruža široko tumačenje obrade osobnih podataka u svrhe znanstvenih istraživanja, uključujući tehnološki razvoj i demonstracije, osnovna istraživanja, primijenjena istraživanja i istraživanja koja se financiraju privatnim sredstvima. Također se prepoznaje važnost prikupljanja podataka u registrima u istraživačke svrhe i moguće poteškoće u točnom utvrđivanju naknadne svrhe obrade osobnih podataka u svrhe znanstvenih istraživanja u trenutku prikupljanja podataka⁹⁵⁵. Zbog toga se Uredbom omogućuje obrada podataka u te svrhe, bez privole ispitanika, pod uvjetom da su uspostavljene odgovarajuće zaštitne mjere.

Važan primjer uporabe podataka u statističke svrhe jesu službene statistike koje prikupe nacionalni zavodi za statistiku i zavodi za statistiku EU-a na temelju nacionalnih zakonodavstava i zakonodavstva EU-a o službenoj statistici. Prema tim zakonodavstvima, građani i poduzeća uglavnom su dužni otkriti podatke odgovarajućim tijelima nadležnima za statistiku. Službenici koji rade u zavodima za statistiku dužni su čuvati

952 Opća uredba o zaštiti podataka, članak 89. stavak 1.

953 *Ibid.*, članak 89. stavak 2.

954 *Ibid.*, uvodna izjava 26.

955 *Ibid.*, uvodne izjave 33., 157. i 159.

poslovnu tajnu. Tu svoju obvezu moraju propisno ispunjavati jer je ona nužna da bi građani imali visoku razinu povjerenja i stavili svoje podatke na raspolaganje tijelima nadležnima za statistiku⁹⁵⁶.

U Uredbi (EZ) br. 223/2009 o europskoj statistici (Uredba o europskoj statistici) sadržana su osnovna pravila zaštite podataka u kontekstu službene statistike, koja se stoga mogu smatrati relevantnima i za odredbe o službenoj statistici na nacionalnoj razini⁹⁵⁷. U Uredbi se zastupa načelo da je za službene statističke aktivnosti potrebna dovoljno jasna pravna osnova⁹⁵⁸.

Primjer: U predmetu *Huber protiv Bundesrepublik Deutschland*⁹⁵⁹ austrijski poduzetnik koji se preselio u Njemačku požalio se da su njemačka tijela prikupljanjem i pohranom osobnih podataka stranih državljana u središnjem registru (AZR), među ostalim u statističke svrhe, prekršile njegova prava na temelju Direktive o zaštiti podataka. Budući da se Direktivom 95/46/EZ namjeravala osigurati odgovarajuća razina zaštite podataka u svim državama članicama, SEU je smatrao da se značenje koncepta nužnosti iz članka 7. točke (e) ne može razlikovati među državama članicama, kako bi se osigurala visoka razina zaštite u EU-u. Stoga je riječ o konceptu koji ima vlastito neovisno značenje unutar prava EU-a i mora se tumačiti tako da u potpunosti odražava cilj Direktive 95/46/EZ. Napominjući da bi za statističke svrhe trebale biti potrebne samo anonimne informacije, SEU je presudio da njemački registar nije u skladu sa zahtjevom nužnosti iz članka 7. točke (e).

U kontekstu **Vijeća Europe** daljnja obrada podataka može se vršiti u znanstvene, povijesne ili statističke svrhe kada je to u javnom interesu te mora podlijeagati odgovarajućim zaštitnim mjerama⁹⁶⁰. Prava ispitanika mogu se ograničiti i prilikom obrade

956 *Ibid.*, članak 90.

957 Uredba (EZ) br. 223/2009 Europskog parlamenta i Vijeća od 11. ožujka 2009. o europskoj statistici i stavljanju izvan snage Uredbe (EZ, Euratom) br. 1101/2008 Europskog parlamenta i Vijeća o dostavi povjerljivih statističkih podataka Statističkom uredu Europskih zajednica, Uredbe Vijeća (EZ) br. 322/97 o statistici Zajednice i Odluke Vijeća 89/382/EEZ, Euratom o osnivanju Odbora za statistički program Europskih zajednica, SL 2009 L 87, kako je izmijenjena Uredbom (EU) 2015/759 Europskog parlamenta i Vijeća od 29. travnja 2015. o izmjeni Uredbe (EZ) br. 223/2009 o europskoj statistici, SL 2015 L 123.

958 To se načelo treba dodatno razraditi u *Eurostatovu Kodeksu prakse*, u kojem će se, u skladu s člankom 11. Uredbe o europskoj statistici, navoditi etičke smjernice o načinu provedbe službene statistike, uključujući pažljivu uporabu osobnih podataka.

959 SEU, C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008.; vidjeti posebno t. 68.

960 Modernizirana Konvencija br. 108, članak 5. stavak 4. točka (b).

podataka u statističke svrhe, pod uvjetom da ne postoji jasan rizik od kršenja njihovih prava i sloboda⁹⁶¹.

Preporuka o statističkim podacima koja je izdana 1997. obuhvaća provedbu statističkih aktivnosti u javnom i privatnom sektoru⁹⁶².

Podaci koje voditelj obrade prikuplja u statističke svrhe ne smiju se upotrebljavati ni u koju drugu svrhu. Podaci prikupljeni u nestatističke svrhe moraju biti dostupni za daljnju uporabu u statističke svrhe. Preporukom o statističkim podacima omogućuje se i prenošenje podataka trećim osobama, pod uvjetom da se to čini isključivo u statističke svrhe. U tim bi slučajevima stranke trebale dogovoriti i zabilježiti opseg zakomite daljnje uporabe u statističke svrhe. Budući da to ne zamjenjuje privolu ispitanika, u nacionalnom zakonodavstvu moraju biti propisane odgovarajuće zaštitne mjere koje bi se po potrebi primjenjivale radi smanjenja rizika od zlouporabe osobnih podataka, kao što je obveza anonimizacije ili pseudonimizacije podataka prije otkrivanja.

Stručnjaci za statistička istraživanja moraju biti obvezani posebnim dužnostima čuvanja poslovne tajne u sklopu nacionalnog zakonodavstva, što je obično slučaj sa službenom statistikom. To se mora proširiti i na ispitivače i druge osobe koje prikupljaju osobne podatke ako su zaposlene na prikupljanju podataka od ispitanika ili drugih osoba.

Ako uporaba osobnih podataka u statističkom istraživanju nije dopuštena zakonom, ispitanici možda trebaju dati privolu za uporabu njihovih podataka, ili barem imati mogućnost prigovora kako bi obrada bila zakonita. Ako ispitivači prikupljaju osobne podatke u statističke svrhe, te osobe moraju biti jasno informirane o tome je li pružanje podataka obvezno prema nacionalnom zakonodavstvu.

Ako statističko istraživanje nije moguće provesti s anonimiziranim podacima, već su nužni osobni podaci, podaci prikupljeni u tu svrhu moraju se anonimizirati što prije. Na temelju rezultata statističkog istraživanja u najmanju ruku ne smije biti moguće identificirati ispitanike, osim ako to jasno ne predstavlja nikakav rizik.

Po završetku statističke analize osobne podatke treba ili izbrisati ili anonimizirati. U tom se slučaju u Preporuci o statističkim podacima savjetuje pohrana

961 *Ibid.*, članak 11. stavak 2.

962 Vijeće Europe, Odbor ministara (1997.), Preporuka Rec(97)18 državama članicama o zaštiti osobnih podataka koji se prikupljaju i obrađuju u statističke svrhe, 30. rujna 1997.

identifikacijskih podataka odvojeno od ostalih osobnih podataka. To na primjer znači da se ključ za kodiranje ili popis sinonima za identifikaciju moraju pohraniti odvojeno od drugih podataka.

9.5. Financijski podaci

Ključne točke

- Iako se financijski podaci ne smatraju osjetljivim podacima u smislu modernizirane Konvencije br. 108 ili Opće uredbe o zaštiti podataka, za njihovu su obradu potrebne posebne zaštitne mjere radi osiguravanja točnosti i sigurnosti podataka.
- Elektronički platni sustavi zahtijevaju ugrađenu zaštitu podataka, odnosno privatnost ili tehničku i integriranu zaštitu podataka.
- U tom području dolazi do posebnih problema sa zaštitom podataka jer treba primjenjivati odgovarajuće mehanizme za autentifikaciju.

Primjer: U predmetu *Michaud protiv Francuske*⁹⁶³ tužitelj, francuski odvjetnik, suprotstavio se svojoj obvezi prijave sumnji povezanih s mogućim aktivnostima pranja novca koje provode njegovi klijenti, na što ga je obvezivalo francusko zakonodavstvo. ESLJP je istaknuo da je zahtijevanje od odvjetnika da upravnim tijelima prijavljuju informacije koje se odnose na drugu osobu, a koje su dobili u službenoj komunikaciji s tom osobom, predstavlja miješanje u pravo odvjetnika na poštovanje njihova dopisivanja i privatnog života prema članku 8. EKLJP-a jer to načelo obuhvaća aktivnosti profesionalne ili poslovne prirode. Međutim, miješanje je bilo u skladu sa zakonom i imalo je legitimnu svrhu, točnije sprečavanje nereda i zločina. Budući da odvjetnici podliježu obvezi prijavljivanja sumnjivih aktivnosti samo u vrlo ograničenim okolnostima, ESLJP je smatrao da je ta obveza proporcionalna. Zaključio je da nije došlo do kršenja članka 8.

⁹⁶³ ESLJP, *Michaud protiv Francuske*, br. 12323/11, 6. prosinca 2012. Vidjeti i ESLJP, *Niemietz protiv Njemačke*, br. 13710/88, 16. prosinca 1992., t. 29., i ESLJP, *Halford protiv Ujedinjene Kraljevine*, br. 20605/92, 25. lipnja 1997., t. 42.

Primjer: U predmetu *M. N. i drugi protiv San Marina*⁹⁶⁴ tužitelj, građanin Italije, sklopio je fiducijarni ugovor s društvom koje je bilo pod istragom. To je značilo da je društvo podvrgnuto pretrazi i zapljeni kopija (elektroničke) dokumentacije. Tužitelj je podnio pritužbu pred sudom u San Marinu tvrdeći da ne postoji poveznica između njega i navodnih kaznenih djela. Međutim, sud je njegovu pritužbu proglasio neprihvatljivom jer on nije bio „zainteresirana stranka“. ESLJP je smatrao da je tužitelj bio u znatno nepovoljnom položaju u pogledu sudske zaštite u odnosu na „zainteresiranu stranku“, no njegovi su podaci svejedno podliježali radnjama pretrage i zapljene. Stoga je ESLJP zaključio da je prekršen članak 8.

Primjer: U predmetu *G. S. B. protiv Švicarske*⁹⁶⁵ pojediniosti o bankovnom računu tužitelja poslani su poreznoj upravi SAD-a na temelju sporazuma o administrativnoj suradnji između Švicarske i SAD-a. ESLJP je zaključio da se tim prijenosom ne krši članak 8. EKLJP-a jer je miješanje u pravo na privatnost tužitelja bilo propisano zakonom, imalo je legitiman cilj te je bilo proporcionalno javnom interesu o kojemu je riječ.

Primjenu općeg okvira za zaštitu podataka (kako je utvrđen u Konvenciji br. 108) na kontekst plaćanja razradilo je **Vijeće Europe** u Preporuci Rec(90)19 iz 1990.⁹⁶⁶ U toj je preporuci razjašnjen opseg zakonitog prikupljanja i uporabe podataka u kontekstu plaćanja, naročito platnim karticama. U njoj se nacionalnim zakonodavcima predlažu detaljni propisi o pravilima u pogledu otkrivanja podataka o plaćanju trećim stranama, o vremenskim ograničenjima za zadržavanje podataka, o transparentnosti, sigurnosti podataka i prekograničnom prijenosu podataka te, naposljetku, o nadzoru i pravnim lijekovima. Vijeće Europe izradilo je Mišljenje o prijenosu poreznih podataka⁹⁶⁷, u kojemu se navode preporuke i pitanja koje je potrebno uzeti u obzir prilikom prijenosa poreznih podataka.

964 ESLJP, *M. N. i drugi protiv San Marina*, br. 28005/12, 7. srpnja 2015.

965 ESLJP, *G. S. B. protiv Švicarske*, br. 28601/11, 22. prosinca 2015.

966 Vijeće Europe, Odbor ministara (1990.), Preporuka br. R(90)19 o zaštiti osobnih podataka koji se upotrebljavaju za plaćanje i druge srodne radnje, 13. rujna 1990.

967 Vijeće Europe, Savjetodavni odbor Konvencije br. 108 (2014.), Mišljenje o utjecaju mehanizama za automatsku međudržavnu razmjenu podataka u upravne i porezne svrhe na zaštitu podataka, 4. lipnja 2014.

ESLJP dopušta prijenos financijskih podataka, točnije pojedinosti o bankovnom računu pojedinca, na temelju članka 8. EKLJP-a ako je to propisano zakonom, ima legitiman cilj i proporcionalno je javnom interesu o kojemu je riječ⁹⁶⁸.

Kad je riječ o **pravu EU-a**, elektronički platni sustavi koji uključuju obradu osobnih podataka moraju biti u skladu s Općom uredbom o zaštiti podataka. Stoga ti sustavi moraju pružati tehničku i integriranu zaštitu podataka. Tehnička zaštita podataka podrazumijeva da je voditelj obrade dužan uspostaviti odgovarajuće tehničke i organizacijske mjere za provedbu načela zaštite podataka. Integrirana zaštita podataka podrazumijeva da voditelj obrade mora osigurati da se zadano obrađuju samo oni osobni podaci koji su nužni u određenu svrhu (vidjeti [dio 4.4.](#)). U kontekstu financijskih podataka SEU je smatrao da preneseni porezni podaci mogu predstavljati osobne podatke⁹⁶⁹. Radna skupina iz članka 29. izdala je povezane smjernice za države članice koje su uključivale kriterije za osiguravanje usklađenosti s propisima o zaštiti podataka prilikom automatske razmjene osobnih podataka u porezne svrhe putem automatiziranih sredstava⁹⁷⁰.

Usto, donesen je niz pravnih instrumenata za uređenje financijskih tržišta i aktivnosti kreditnih institucija i investicijskih društava⁹⁷¹. Ostali pravni instrumenti pomažu u suzbijanju trgovanja na temelju povlaštenih informacija i manipuliranja tržištem⁹⁷². Najvažnija su područja koja utječu na zaštitu podataka:

- zadržavanje zapisa o financijskim transakcijama,
- prijenos osobnih podataka u treće zemlje,

968 ESLJP, *G. S. B. protiv Švicarske*, br. 28601/11, 22. prosinca 2015.

969 SEU, C-201/14, *Smăranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. listopada 2015., t. 29.

970 Radna skupina za zaštitu podataka iz članka 29. (2015.), *Izjava Radne skupine za zaštitu podataka iz članka 29. o automatskim međudržavnim razmjenama osobnih podataka u porezne svrhe*, WP 230.

971 Direktiva 2014/65/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištu financijskih instrumenata i izmjeni Direktive 2002/92/EZ i Direktive 2011/61/EU, SL 2014 L 173; Uredba (EU) br. 600/2014 Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Uredbe (EU) br. 648/2012, SL 2014 L 173; Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ, SL 2013 L 176.

972 Uredba (EU) br. 596/2014 Europskog parlamenta i Vijeća od 16. travnja 2014. o zlouporabi tržišta (Uredba o zlouporabi tržišta) te stavljanju izvan snage Direktive 2003/6/EZ Europskog parlamenta i Vijeća i direktiva Komisije 2003/124/EZ, 2003/125/EZ i 2004/72/EZ, SL 2014 L 173.

- snimanje telefonskih razgovora ili elektroničke komunikacije, uključujući ovlaštenje nadležnih tijela da zatraže zapise o telefonskom i podatkovnom prometu,
- otkrivanje osobnih informacija, uključujući objavu sankcija,
- ovlaštenje nadležnih tijela da provode nadzor i istrage, uključujući terenske preglede i ulazak u privatne prostorije radi oduzimanja dokumenata,
- mehanizmi za prijavu kršenja, npr. programi prijavljivanja nepravilnosti (zviždači), te
- suradnja nadležnih tijela država članica i Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala (ESMA).

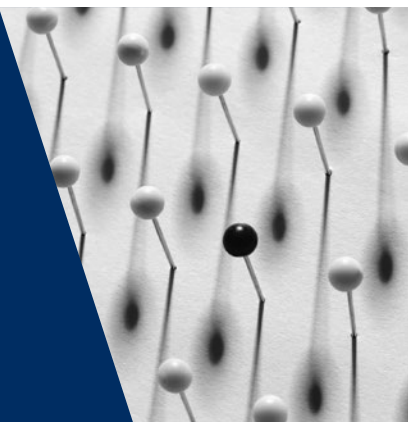
I druga su pitanja u tim područjima posebno obrađena, uključujući prikupljanje podataka o financijskom statusu ispitanika⁹⁷³ ili prekograničnim plaćanjima putem bankovnih prijenosa, što neizbježno dovodi do protoka osobnih podataka⁹⁷⁴.

973 Uredba (EZ) br. 1060/2009 Europskog parlamenta i Vijeća od 16. rujna 2009. o agencijama za kreditni rejting, SL 2009 L 302, naknadno izmijenjena Direktivom 2014/51/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o izmjeni direktiva 2003/71/EZ i 2009/138/EZ te uredbi (EZ) br. 1060/2009, (EU) br. 1094/2010 i (EU) br. 1095/2010 u pogledu ovlasti Europskog nadzornog tijela (Europskog nadzornog tijela za osiguranje i strukovno mirovinsko osiguranje) i Europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), SL 2014 L 153; Uredba (EU) br. 462/2013 Europskog parlamenta i Vijeća od 21. svibnja 2013. o izmjeni Uredbe (EZ) br. 1060/2009 o agencijama za kreditni rejting, SL 2013 L 146.

974 Direktiva 2007/64/EZ Europskog parlamenta i Vijeća od 13. studenoga 2007. o platnim uslugama na unutarnjem tržištu i o izmjeni direktiva 97/7/EZ, 2002/65/EZ, 2005/60/EZ i 2006/48/EZ te stavljanju izvan snage Direktive 97/5/EZ, SL 2007 L 319, kako je izmijenjena Direktivom 2009/111/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o izmjeni direktiva 2006/48/EZ, 2006/49/EZ i 2007/64/EZ vezano za banke povezane sa središnjim institucijama, određene stavke jamstvenog kapitala, velike izloženosti, nadzorne aranžmane i upravljanje u kriznim situacijama, SL 2009 L 302.

10

Suvremeni izazovi u području zaštite osobnih podataka



Digitalno doba, ili doba informacijskih tehnologija, obilježeno je sveopćom upotrebom računala, interneta i digitalnih tehnologija. Ono uključuje prikupljanje i obradu golemih količina podataka, uključujući i osobne podatke. Prikupljanje i obrada osobnih podataka u globaliziranom gospodarstvu podrazumijevaju rast u području prekograničnih prijenosa podataka. Takva obrada nosi značajne i vidljive prednosti u svakodnevnom životu: internetske tražilice olakšavaju pristup velikim količinama informacija i znanja, društvene mreže omogućuju ljudima diljem svijeta da komuniciraju, izražavaju svoja mišljenja i prikupljaju potporu za društvene, ekološke i političke pokrete, a tvrtke i potrošači ostvaruju korist od učinkovitih marketinških metoda koje pokreću gospodarstvo. Tehnologija i obrada osobnih podataka također su neizostavni alati za borbu nacionalnih tijela protiv kaznenih djela i terorizma. Jednako tako tzv. „veliki podaci“, odnosno prikupljanje, pohrana i analiza velikih količina informacija radi utvrđivanja uzoraka i predviđanja ponašanja, „mogu biti izvor značajne vrijednosti za društvo te povećati produktivnost, učinkovitost javnog sektora i društveno sudjelovanje“⁹⁷⁵.

Unatoč brojnim prednostima, digitalno doba donosi i određene izazove za privatnost i zaštitu podataka jer se prikupljaju i obrađuju velike količine osobnih podataka na sve složenije i netransparentne načine. Tehnološki napredak doveo je do razvoja golemih podatkovnih skupova koji se mogu jednostavno unakrsno provjeravati

⁹⁷⁵ Vijeće Europe, Savjetodavni odbor Konvencije br. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data* (Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka), T-PD(2017)01, Strasbourg, 23. siječnja 2017.

i dalje analizirati kako bi se otkrili uzorci ili donosile odluke na temelju algoritama, koji mogu pružiti posve nov uvid u ljudske navike i privatni život⁹⁷⁶.

Nove su tehnologije moćne i mogu biti posebno opasne ako dospiju u pogrešne ruke. Državna tijela koja provode aktivnosti masovnog nadzora i upotrebljavaju te tehnologije primjer su značajnog učinka koji te tehnologije mogu imati na prava pojedinaca. Informacije koje je Edward Snowden otkrio 2013. o provođenju opsežnih programa nadzora interneta i telefona u obavještajnim agencijama nekih američkih saveznih država izazvale su veliku zabrinutost o opasnostima koje aktivnosti nadzora nose za privatnost, demokratsko upravljanje i slobodu izražavanja. Masovni nadzor i tehnologije koje omogućuju globaliziranu pohranu i obradu osobnih podataka i skupni pristup podacima mogli bi narušiti same temelje prava na privatnost⁹⁷⁷. Usto, mogli bi imati negativan učinak na političku kulturu i neželjene posljedice za demokraciju, kreativnost i inovacije⁹⁷⁸. Već i sam strah da bi država mogla neprestano pratiti i analizirati njihovo ponašanje i postupke može građane odvratiti od izražavanja stavova o određenim pitanjima i dovesti do povećanog opreza⁹⁷⁹. Ti su izazovi potaknuli niz javnih tijela, istraživačkih centara i organizacija civilnog društva da analiziraju moguće učinke novih tehnologija na društvo. Europski nadzornik za zaštitu podataka pokrenuo je 2015. nekoliko inicijativa koje su bile usmjerene na procjenu učinka velikih podataka i interneta stvari (engl. *Internet of Things*) na etičnost. Među ostalim, osnovao je Savjetodavnu skupinu za etička pitanja, koja za cilj ima poticanje „otvorene i informirane rasprave o digitalnoj etici, što Europskoj uniji omogućava uočavanje prednosti tehnologije za društvo i gospodarstvo, uz istodobno jačanje prava i slobode pojedinaca, posebice njihova prava na privatnost i zaštitu podataka”⁹⁸⁰.

976 Europski parlament (2017.), *Rezolucija o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon* (P8_TA-PROV(2017)0076), Strasbourg, 14. ožujka 2017.

977 Vidjeti UN, Opća skupština, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (Izvešće posebnog izvjestitelja o promicanju i zaštiti ljudskih prava i temeljnih sloboda u borbi protiv terorizma), Ben Emmerson, A/69/397, 23. rujna 2014, st. 59. Vidjeti i ESLJP, *Factsheet on Mass surveillance* (Informativni list o masovnom nadzoru), srpanj 2017.

978 EDPS (2015.), *Svladavanje izazova velikih podataka, Mišljenje 7/2015*, Bruxelles, 19. studenoga 2015.

979 Vidjeti posebno SEU, spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr.* i *Kärntner Landesregierung i dr.* [VV], 8. travnja 2014., t. 37.

980 EDPS, Odluka od 3. prosinca 2015. o uspostavi vanjske savjetodavne skupine za etičke dimenzije zaštite podataka („Savjetodavna skupina za etička pitanja”), 3. prosinca 2015., uvodna izjava 5.

Obrada osobnih podataka snažan je alat i u rukama korporacija. Ona danas može otkriti detaljne informacije o zdravlju ili financijskoj situaciji osobe, koje zatim korporacije upotrebljavaju kako bi donosile važne odluke za pojedince, poput premija zdravstvenog osiguranja koje će se primjenjivati na njih ili pak njihove kreditne sposobnosti. Metode obrade podataka mogu utjecati i na demokratske procese kada ih političari ili korporacije upotrebljavaju da bi utjecali na izbore, primjerice „mikrociljanjem“ poruka glasačima. Drugim riječima, iako se privatnost prvobitno smatrala pravom na zaštitu pojedinaca od neopravdanog miješanja tijela javne vlasti, u novije doba ona može biti ugrožena i ovlastima privatnih dionika. Zbog toga se postavlja pitanje o uporabi tehnologije i prediktivne analize u odlukama koje utječu na svakodnevni život pojedinaca te se potvrđuje potreba za osiguravanjem toga da se pri svakoj obradi osobnih podataka poštuju zahtjevi temeljnih prava.

Zaštita podataka neraskidivo je povezana s tehnološkim, društvenim i političkim promjenama. Stoga je nemoguće sastaviti cjelovit popis izazova koji bi se mogli javiti u budućnosti. U ovom se poglavlju razmatraju odabrana područja koja se odnose na velike podatke, internetske društvene mreže i jedinstveno digitalno tržište EU-a. Nije riječ o iscrpnoj procjeni tih područja sa stajališta zaštite podataka, nego se ističu brojni mogući međuodnosi novih ili izmijenjenih ljudskih aktivnosti i zaštite podataka.

10.1. Veliki podaci, algoritmi i umjetna inteligencija

Ključne točke

- Radikalne inovacije u području IKT-a oblikuju nov način života u sklopu kojega su društveni odnosi, poslovanje, privatne i javne usluge međusobno digitalno povezani, što dovodi do stvaranja sve veće količine podataka, od kojih su mnogi osobni podaci.
- Vlade, poduzeća i građani sve više djeluju u gospodarstvu utemeljenom na podacima, u kojemu su sami podaci postali vrijedna imovina.
- Koncept velikih podataka odnosi se na podatke i njihovu analitiku.
- Osobni podaci koji se obrađuju u sklopu analitike velikih podataka potpadaju pod zakonodavstvo EU-a i Vijeća Europe.

- Odstupanja od propisa i prava na zaštitu podataka ograničena su na odabrana prava i određene situacije u kojima bi se provođenje prava pokazalo nemogućim ili bi zahtijevalo nerazmjeran napor voditelja obrade.
- Potpuno automatizirano donošenje odluka u pravilu je zabranjeno, osim u određenim slučajevima.
- Svijest među pojedincima i njihova kontrola ključni su za osiguravanje provedbe prava.

U svijetu koji je sve više digitaliziran svaka aktivnost ostavlja digitalni trag koji se može prikupiti, obraditi i procijeniti ili analizirati. Zahvaljujući novim informacijskim i komunikacijskim tehnologijama sve se više podataka prikuplja i bilježi⁹⁸¹. Donekadno nijednom tehnologijom nije bilo moguće analizirati ili procijeniti količinu podataka ili izvesti korisne zaključke. Podataka je, jednostavno, bilo previše da bi se mogli procijeniti, bili su previše složeni, loše strukturirani i prebrzo su se prenosili da bi se mogli utvrditi trendovi i navike.

10.1.1. Definicije velikih podataka, algoritama i umjetne inteligencije

Veliki podaci

Pojam „velikih podataka“ (engl. *big data*) jedan je od popularnih izraza današnjice, a može označavati nekoliko koncepata ovisno o kontekstu. Obično obuhvaća „sve veću tehnološku mogućnost prikupljanja, obrade i izdvajanja novih i prediktivnih saznanja iz velike količine, brzine i raznovrsnosti podataka“⁹⁸². Koncept velikih podataka stoga obuhvaća i same podatke i podatkovnu analitiku.

Podaci dolaze iz različitih vrsta **izvora**, koji uključuju osobe i njihove osobne podatke, uređaje ili senzore, informacije o klimi, satelitske snimke, digitalne fotografije i videozapise ili GPS signale. Međutim, velik dio podataka i informacija čine osobni podaci, odnosno ime, fotografija, adresa e-pošte, bankovni podaci, podaci za GPS

981 Europska komisija, Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, „Prema rastućem gospodarstvu temeljenom na podacima“, COM(2014) 442 final, Bruxelles, 2. srpnja 2014.

982 Vijeće Europe, Savjetodavni odbor Konvencije br. 108, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 2.; Europska komisija, Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, „Prema rastućem gospodarstvu temeljenom na podacima“, COM(2014) 442 final, Bruxelles, 2. srpnja 2014., str. 4.; Međunarodna telekomunikacijska unija (2015.), Preporuka Y.3600. Veliki podaci: zahtjevi i mogućnosti utemeljeni na računalstvu u oblaku.

praćenje, objave na internetskim stranicama društvenih mreža, medicinski podaci ili IP adresa računala⁹⁸³.

Pojam „veliki podaci” odnosi se i na **obradu**, analizu i procjenu skupova podataka i dostupnih informacija, odnosno prikupljanje korisnih informacija u svrhu analize velikih podataka. To znači da se prikupljeni podaci i informacije mogu upotrijebiti u svrhe koje se razlikuju od prvotno predviđenih, primjerice za statističke trendove ili za posebno prilagođene usluge poput oglašavanja. U slučajevima u kojima postoje tehnologije za prikupljanje, obradu i procjenu velikih podataka zapravo se svaka vrsta informacija može kombinirati i ponovno procijeniti: financijske transakcije, kreditna sposobnost, medicinsko liječenje, osobna potrošnja, stručna djelatnost, praćenje i odabrani putovi, uporaba interneta, elektroničkih kartica i pametnih telefona te videonadzor ili nadzor komunikacija. Analizom velikih podataka dobiva se nova kvantitativna dimenzija podataka koja se može procijeniti i iskoristiti u stvarnom vremenu, primjerice radi pružanja prilagođenih usluga potrošačima.

Algoritmi i umjetna inteligencija

Umjetna inteligencija (UI) odnosi se na inteligenciju strojeva koji djeluju kao „inteligentni subjekti”. Kao inteligentni subjekti, određeni uređaji uz pomoć softvera mogu opažati svoje okruženje i poduzimati radnje na temelju algoritama. Pojam UI-ja primjenjuje se kada stroj oponaša „kognitivne” funkcije poput učenja i rješavanja problema, koje se obično povezuju s ljudima⁹⁸⁴. Da bi oponašali donošenje odluka, moderne tehnologije i softveri upotrebljavaju algoritme koji omogućuju uređajima da donose „automatizirane odluke”. Algoritam se najbolje može opisati kao postupni proces izračuna, obrade podataka, procjene i automatiziranog rasuđivanja i donošenja odluka.

Slično kao i analitika velikih podataka, umjetna inteligencija i njezino automatizirano donošenje odluka zahtijevaju kompiliranje i obradu velikih količina podataka. Ti podaci mogu proizlaziti iz samog uređaja (toplina kočnica, gorivo itd.) ili okruženja. Primjerice, izrada profila postupak je koji se može temeljiti na automatiziranom donošenju odluka u skladu s unaprijed određenim uzorcima ili čimbenicima.

983 „Reforma zaštite podataka u EU-u i veliki podaci”, *Informativni list Komisije EU-a*, Vijeće Europe, Savjetodavni odbor Konvencije br. 108, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 2.

984 Russel, S. i Norvig, P., *Artificial Intelligence: A Modern Approach (2nd ed.)*, Upper Saddle River, New Jersey: Prentice Hall, 2003., str. 27., 32.-58., 968.-972.; Russel, S. i Norvig, P., *Artificial Intelligence: A Modern Approach (3rd ed.)*, Upper Saddle River, New Jersey: Prentice Hall, 2009., str. 2.

Primjer: Izrada profila i ciljano oglašavanje

Izrada profila na temelju velikih podataka uključuje utvrđivanje uzoraka koji odražavaju „obilježja određenog tipa osobnosti“, primjerice kada tvrtke za internetsku prodaju na temelju informacija prikupljenih od proizvoda koje je korisnik prethodno stavio u košaricu za kupovinu predlažu druge proizvode uz izraz: „Također bi vam se moglo svidjeti...“ Što je više podataka dostupno, to je slika jasnija. Primjerice, pametni telefoni važan su upitnik koji pojedinci ispunjavaju pri svakoj upotrebi, bilo svjesno bilo nesvjesno.

Suvremena psihografija, znanost koja proučava osobnosti, temelji se na metodi OCEAN prema kojoj određuje pojedini tip osobnosti. Pet osnovnih dimenzija osobnosti (engl. *Big Five*) odnosi se na otvorenost prema iskustvima (engl. *Openness*; koliko je osoba otvorena prema novostima), savjesnost (engl. *Conscientiousness*; koliko je osoba sklona perfekcionizmu), ekstravertiranost (engl. *Extraversion*; koliko je osoba društvena), ugodnost (engl. *Agreeableness*; koliko je osoba ugodna) i neurotičnost (engl. *Neuroticism*; koliko je osoba osjetljiva). Na temelju tih informacija moguće je izraditi profil dotične osobe, njezinih potreba i strahova, ponašanja itd. Profil se zatim nadopunjuje drugim informacijama o osobi koje se dobivaju iz svih dostupnih izvora – od posrednika za podatke, s društvenih mreža (uključujući oznake „Sviđa mi se“ za objave i objavljene fotografije), iz glazbe koja se sluša putem interneta ili GPS podataka ili podataka o praćenju.

Skupovi profila koji se izrađuju na temelju metoda analize velikih podataka tada se uspoređuju kako bi se utvrdili slični uzorci i oblikovali skupovi osobnosti. Stoga se informacije o ponašanju i stavovima određenih osobnosti preokreću. Zahvaljujući pristupu velikim podacima i njihovoj uporabi test osobnosti se preokreće te se informacije o ponašanju i stavovima sada rabe za opis osobnosti pojedinca. Kombiniranjem informacija o oznakama „Sviđa mi se“ na društvenim mrežama, podataka o praćenju, glazbe koja se sluša ili pogledanih filmova dobiva se jasna slika osobnosti pojedinca, a tvrtkama se omogućuje da prenose prilagođene oglase i/ili informacije u skladu s tipom „osobnosti“ te osobe. Povrh svega, te se informacije mogu obrađivati u stvarnom vremenu⁹⁸⁵.

⁹⁸⁵ Metodama obrade i novim softverom u stvarnom se vremenu procjenjuju informacije o tome što se nekoj osobi sviđa, što gleda prilikom internetske kupnje ili što dodaje u košaricu za kupovinu te se mogu predlagati „proizvodi“ koji bi joj se mogli svidjeti na temelju prikupljenih informacija.

10.1.2. Odvagivanje koristi i rizika velikih podataka

Suvremene metode obrade mogu podnijeti velike količine podataka, brzo uvođenje novih podataka, pružiti obradu informacija u stvarnom vremenu zahvaljujući kratkom vremenu odaziva (čak i u slučaju složenih zahtjeva), omogućiti višestruke i istovremene zahtjeve i analizirati različite vrste informacija (fotografije, tekstove ili brojeve). Te tehnološke inovacije omogućuju strukturiranje, obradu i procjenu skupova podataka i informacija u stvarnom vremenu⁹⁸⁶. Eksplozivnim povećanjem količine podataka koji su dostupni i koji se analiziraju mogu se postići rezultati koji bi bili nemogući u slučaju analize manjeg opsega. Veliki podaci pomogli su u razvoju novog područja poslovanja u sklopu kojega se nove usluge mogu početi pružati i poduzećima i pojedincima. Vrijednost osobnih podataka građana EU-a mogla bi narasti na gotovo 1 trilijun € godišnje do 2020.⁹⁸⁷ Stoga veliki podaci mogu pružiti nove **moćnosti** koje proizlaze iz procjene skupnih podataka za nove društvene, gospodarske ili znanstvene uvide koji mogu koristiti pojedincima, poduzećima i vladama⁹⁸⁸.

Analitika velikih podataka može otkriti uzorke među različitim izvorima i skupovima podataka, koji mogu pružiti korisne uvide u područja poput znanosti i medicine. Primjerice, to je slučaj s područjima poput zdravstva, sigurnosti hrane, inteligentnih sustava prijevoza, energetske učinkovitosti ili urbanističkog planiranja. Takva analiza informacija u stvarnom vremenu može se upotrijebiti za poboljšanje uvedених sustava. U istraživanjima se novi uvidi mogu ostvariti kombiniranjem velike količine podataka i statističkih procjena, posebice u disciplinama u kojima su se do sada podaci uvelike ručno procjenjivali. Mogu se razviti nove terapije prilagođene pojedinim pacijentima na temelju usporedbe sa skupom dostupnih informacija. Tvrtke se nadaju da će im analiza velikih podataka omogućiti ostvarenje konkurentne

986 Razvoj softvera za obradu velikih količina podataka još je u začetima. Međutim, nedavno su razvijeni analitički programi, osobito za analizu skupnih podataka i informacija u stvarnom vremenu povezanih s aktivnostima pojedinaca. Mogućnost strukturiranog analiziranja i obrađivanja velike količine podataka omogućila je novi oblik izrade profila i ciljanog oglašavanja. Europska komisija, Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija „Prema rastućem gospodarstvu temeljenom na podacima“, COM(2014) 442 final, Bruxelles, 2. srpnja 2014. ; Informativni list Komisije EU-a, „Reforma zaštite podataka u EU-u i veliki podaci“ i Vijeće Europe, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 2.

987 Informativni list Komisije EU-a, „Reforma zaštite podataka u EU-u i veliki podaci“.

988 Međunarodna konferencija povjerenika za zaštitu podataka i privatnost (2014.), Rezolucija o velikim podacima i Europska komisija, Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, „Prema rastućem gospodarstvu temeljenom na podacima“, COM(2014) 442 final, Bruxelles, 2. srpnja 2014., str. 2.; Informativni list Komisije EU-a, „Reforma zaštite podataka u EU-u i veliki podaci“ te Vijeće Europe, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 1.

prednosti, donijeti moguće uštede i stvoriti nova područja poslovanja putem izravne, individualizirane usluge usmjerene na korisnike. Državne agencije nadaju se da će ostvariti poboljšanja u kaznenom pravosuđu. U Komisijinoj Strategiji jedinstvenog digitalnog tržišta za Europu prepoznat je potencijal tehnologija i usluga koje pokreću podaci te velikih podataka da djeluju kao pokretači gospodarskog rasta, inovacija i digitalizacije u EU-u⁹⁸⁹. Međutim, veliki podaci nose i određene **rizike** koji se obično povezuju s količinom, brzinom i raznolikošću obrađenih podataka. Riječ je, zapravo, o količini obrađenih podataka, broju i raznovrsnosti podataka odnosno brzini obrade podataka. Posebna pitanja zaštite podataka javljaju se kada se analitika velikih podataka upotrebljava na velikim skupovima podataka radi izdvajanja novih i prediktivnih saznanja u svrhe donošenja odluka o pojedincima i/ili skupinama⁹⁹⁰. Rizici za zaštitu podataka i privatnost povezani s velikim podacima istaknuti su u mišljenjima Radne skupine iz članka 29., rezolucijama Europskog parlamenta i dokumentima s politikama Vijeća Europe⁹⁹¹.

Rizici mogu uključivati pogrešno postupanje s velikim podacima među onima koji imaju pristup skupnim informacijama, u smislu manipulacije, diskriminacije ili ugnjetavanja pojedinaca ili pojedinih skupina u društvu⁹⁹². Kada se skupovi osobnih podataka ili informacija o ponašanju pojedinaca prikupljanju, obrađuju i procjenjuju, njihovo iskorištavanje može dovesti do značajnih kršenja temeljnih prava i sloboda izvan prava na privatnost. Mjerenje točnog razmjera u kojemu to može utjecati na privatnosti i osobne podatke nije moguće. Europski parlament utvrdio je da nedostaje metodologija za procjenu cjelokupnog učinka velikih podataka na temelju dokaza, no postoje dokazi koji ukazuju na to da analitika velikih podataka može imati značajan horizontalni utjecaj na javni i privatni sektor⁹⁹³.

989 Rezolucija Europskog parlamenta od 14. ožujka 2017. o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon (2016/2225 (INI)).

990 Vijeće Europe, Savjetodavni odbor Konvencije br. 108, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 2.

991 Primjerice, vidjeti EDPS (2015.), Svladavanje izazova velikih podataka, Mišljenje 7/2015, 19. studenoga 2015.; EDPS (2016.), Dosljedno jačanje temeljnih prava u doba velikih podataka, Mišljenje 8/2016, 23. rujna 2016.; Europski parlament (2016.), Rezolucija o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon (P8_TA(2017)0076), Strasbourg, 14. ožujka 2017.; Vijeće Europe, Savjetodavni odbor Konvencije br. 108, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, T-PD(2017)01, Strasbourg, 23. siječnja 2017.

992 Međunarodna konferencija povjerenika za zaštitu podataka i privatnost (2014.), Rezolucija o velikim podacima.

993 Rezolucija Europskog parlamenta od 14. ožujka 2017. o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon (2016/2225 (INI)).

Opća uredba o zaštiti podataka sadržava odredbe o pravu da se na pojedinca ne odnosi odluka koja se temelji na automatiziranoj obradi, uključujući izradu profila⁹⁹⁴. Pitanje privatnosti javlja se kada ostvarivanje prava na prigovor zahtijeva ljudsku intervenciju, kojom se ispitanicima omogućuje da izraze svoje stajalište i ospore odluku⁹⁹⁵. Iz toga mogu proizaći izazovi u pogledu osiguravanja odgovarajuće razine zaštite osobnih podataka ako, primjerice, ljudska intervencija nije moguća ili ako su algoritmi presloženi, a količina podataka prevelika da bi se pojedincima pružila obrazloženja za određene odluke i/ili da bi im se pružile prethodne informacije kako bi se ishodila njihova privola. Primjer upotrebe umjetne inteligencije i automatiziranog donošenja odluka vidljiv je u novim pojavama u području zahtjeva za hipoteke ili tijekom procesa zapošljavanja. Zahtjevi i prijave odbijaju se ili odbacuju na temelju činjenice da podnositelji ne ispunjavaju predodređene parametre ili čimbenike.

10.1.3. Problemi povezani sa zaštitom podataka

U kontekstu zaštite podataka osnovni se problemi s jedne strane odnose na količinu i raznolikost osobnih podataka koji se obrađuju, a s druge na obradu i njezine rezultate. Uvođenje složenih algoritama i softvera za pretvorbu skupnih podataka u izvor za donošenje odluka posebno utječe na pojedince i skupine, ponajviše u slučaju izrade profila ili označavanja, te u konačnici dovodi do brojnih problema zaštite podataka⁹⁹⁶.

Utvrđivanje voditelja obrade i izvršitelja obrade te njihove odgovornosti

Veliki podaci i umjetna inteligencija dovode do niza pitanja u vezi s utvrđivanjem voditelja obrade i izvršitelja obrade te njihovom odgovornošću: kada se prikuplja i obrađuje toliko velika količina podataka, tko je vlasnik podataka? Kada podatke obrađuju inteligentni strojevi i softver, tko je voditelj obrade? Koje su točne odgovornosti svakog dionika obrade? U koje se svrhe mogu upotrebljavati veliki podaci?

Problem odgovornosti u kontekstu UI-ja dodatno će se otežati kada UI donese odluku utemeljenu na obradi podataka koju sam razvije. Opća uredba o zaštiti podataka pruža pravni okvir za odgovornost voditelja i izvršitelja obrade podataka.

994 Opća uredba o zaštiti podataka, članak 22.

995 *Ibid.*, članak 22. stavak 3.

996 Vijeće Europe, Savjetodavni odbor Konvencije br. 108, Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka, 23. siječnja 2017., str. 2.

Nezakonitom obradom osobnih podataka nastaje odgovornost za voditelja i izvršitelja obrade podataka⁹⁹⁷. Pri uporabi umjetne inteligencije i automatiziranog donošenja odluka postavlja se pitanje o tome tko snosi odgovornost za povrede privatnosti ispitanika kada se složenost i količina obrađenih podataka ne mogu točno utvrditi. U slučajevima u kojima se umjetna inteligencija i algoritmi smatraju proizvodima javlja se problem osobne odgovornosti, koja je uređena Općom uredbom o zaštiti podataka, i odgovornosti za proizvod, koja nije uređena Uredbom⁹⁹⁸. Za to su potrebni propisi o odgovornosti kako bi se ispunila praznina između osobne odgovornosti i odgovornosti za proizvod, primjerice za robotiku i UI, uključujući automatizirano donošenje odluka⁹⁹⁹.

Utjecaj na načela zaštite podataka

Priroda, analiza i upotreba gore opisanih velikih podataka dovode u pitanje primjenu određenih tradicionalnih, temeljnih načela europskog zakonodavstva o zaštiti podataka¹⁰⁰⁰. Izazovi se uglavnom odnose na načela zakonitosti, smanjenja količine podataka, ograničenja svrhe i transparentnosti.

Sukladno načelu smanjenja količine podataka, osobni podaci moraju biti prikladni, relevantni i ograničeni na ono što je nužno u svrhe u koje se obrađuju. Međutim, poslovni model velikih podataka mogao bi biti sušta suprotnost smanjenju količine podataka s obzirom na to da zahtijeva sve više i više podataka, često u neodređene svrhe.

To se odnosi i na načelo ograničenja svrhe, prema kojem se podaci moraju obrađivati u određene svrhe i ne smiju se upotrebljavati u svrhe koje nisu u skladu s prvobitnom svrhom prikupljanja, osim ako se takva obrada temelji na nekoj pravnoj osnovi, poput, među ostalim, privole ispitanika (vidjeti [dio 4.1.1.](#)).

997 Opća uredba o zaštiti podataka, članci od 77. do 79. i članak 82.

998 Europski parlament, europska Pravila građanskog prava o robotici, Opća uprava za unutarnju politiku, (listopad 2016), str. 14.

999 Govor Roberta Viole (dostupan na engleskom jeziku) na medijskom seminaru o europskim zakonima o robotici u Europskom parlamentu. (SPEECH 16/02/2017); objava Europskog parlamenta (dostupna na engleskom jeziku) o zahtjevu Komisiji za prijedlog Pravila o građanskopravnoj odgovornosti za robotiku i umjetnu inteligenciju.

1000 Vijeće Europe, *Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka*, T-PD (2017) 01, Strasbourg, 23. siječnja 2017.

Naposljetku, veliki podaci dovode u pitanje i načelo točnosti podataka s obzirom na to da se u takvim primjenama najčešće prikupljaju podaci iz različitih izvora bez mogućnosti provjere i/ili osiguravanja točnosti prikupljenih podataka¹⁰⁰¹.

Posebna pravila i prava

Opće je pravilo da osobni podaci koji se obrađuju u sklopu analitike velikih podataka potpadaju pod područje primjene zakonodavstva o zaštiti podataka. Unatoč tome, u pravu EU-a i Vijeća Europe uvedena su posebna pravila ili odstupanja u određenim slučajevima koji se odnose na složenu algoritamsku obradu podataka.

U sklopu prava Vijeća Europe moderniziranom Konvencijom br. 108 ispitanicima se dodjeljuju nova prava kako bi se osigurao njihov učinkovitiji nadzor nad vlastitim osobnim podacima u dobu velikih podataka. Primjerice, to je slučaj s člankom 9. stavkom 1. točkama (a), (c) i (d) modernizirane Konvencije, koje se odnose na pravo da se na osobu ne primjenjuje odluka koja značajno utječe na nju, a koja se temelji na automatiziranoj obradi podataka, bez uzimanja u obzir stajališta te osobe; na pravo da se na zahtjev dobiju informacije o razlozima za obradu podataka ako se rezultati takve obrade odnose na nju; te na pravo na prigovor. Ostale odredbe modernizirane Konvencije br. 108, ponajviše odredbe o transparentnosti i dodatnim obvezama, dopunjavaju zaštitni mehanizam uspostavljen moderniziranom Konvencijom br. 108 za suočavanje s izazovima digitalnih tehnologija.

Osim u slučajevima iz članka 23. OUZP-a, pravom Unije mora se osigurati **transparentnost** svake obrade osobnih podataka. Ona je posebno važna u pogledu internetskih usluga i drugih složenih oblika automatizirane obrade podataka, poput uporabe algoritama za donošenje odluka. U tom kontekstu, svojstva sustava za obradu podataka moraju ispitanicima omogućiti da uistinu razumiju što se događa s njihovim podacima. Da bi se osigurala poštena i transparentna obrada, Općom uredbom o zaštiti podataka od voditelja obrade zahtijeva se da ispitaniku pruži smislene informacije o logici automatiziranog donošenja odluka, uključujući izradu profila¹⁰⁰².

U Preporuci o zaštiti i promicanju prava na slobodu izražavanja i prava na privatni život u pogledu mrežne neutralnosti Odbor ministara Vijeća Europe preporučio je da pružatelji internetskih usluga „pružaju korisnicima jasne, potpune i javno dostupne

1001 EDPS (2016.), *Dosljedno jačanje temeljnih prava u doba velikih podataka*, Mišljenje 8/2016, 23. rujna 2016., str. 8.

1002 Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (f).

informacije o svim praksama upravljanja prometom koje bi mogle utjecati na pristup korisnika sadržaju, aplikacijama ili uslugama ili njihovu distribuciju¹⁰⁰³. Izvješća o praksama upravljanja prometom koje sastavljaju nadležna tijela u svim državama članicama trebaju se pripremiti otvoreno i transparentno te besplatno staviti na raspolaganje javnosti¹⁰⁰⁴.

Voditelji obrade moraju **obavijestiti** ispitanike – i kada su podaci prikupljeni od njih i kada nisu – ne samo o točnim informacijama o prikupljenim podacima i predviđenoj obradi (vidjeti [dio 6.1.1.](#)) nego, po potrebi, i o postojanju automatiziranih postupaka donošenja odluka, uključujući „smislene informacije o tome o kojoj je logici riječ”¹⁰⁰⁵, ciljeve i moguće posljedice takvih procesa. U Općoj uredbi o zaštiti podataka pojašnjava se i (samo u slučajevima u kojima osobni podaci nisu dobiveni od ispitanika) da voditelj obrade nije dužan pružiti ispitaniku takve informacije ako je „pružanje takvih informacija nemoguće [...] ili bi zahtijevalo nerazmjerne napore”¹⁰⁰⁶. Međutim, kako ističe Radna skupina iz članka 29. u Smjernicama o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679, složenost obrade sama po sebi ne bi smjela spriječiti voditelja obrade podataka da ispitaniku pruži jasna obrazloženja ciljeva i analitike koja je upotrijebljena za obradu podataka¹⁰⁰⁷.

Prava ispitanika na **pristup** vlastitim osobnim podacima te njihov **ispravak** i **brisanje**, kao i pravo na **ograničenje** obrade, ne sadrže slično izuzeće. Međutim, obveza voditelja obrade podataka da obavijesti ispitanika o svakom ispravku ili brisanju njegovih osobnih podataka (vidjeti [dio 6.1.4.](#)) može se ukinuti ako se takvo obavješćivanje „pokaže nemogućim ili zahtijeva nerazmjeran napor”¹⁰⁰⁸.

Ispitanici također, sukladno članku 21. OUZP-a (vidjeti [dio 6.1.6.](#)), imaju pravo na **prigovor** na svaku obradu svojih osobnih podataka, među ostalim i u slučaju analitike velikih podataka. Iako se voditelji obrade mogu izuzeti iz te obveze ako mogu dokazati prevladavajuće legitimne interese, nemaju pravo na takvo izuzeće u slučaju obrade u svrhe direktnog marketinga.

1003 Vijeće Europe, Odbor ministara (2016.), Preporuka CM/Rec(2016)1 Odbora ministara državama članicama o zaštiti i promicanju prava na slobodu izražavanja i prava na privatni život u pogledu mrežne neutralnosti, 13. siječnja 2016., st. 5.1.

1004 *Ibid.*, st. 5.2.

1005 Opća uredba o zaštiti podataka, članak 13. stavak 2. točka (f) i članak 14. stavak 2. točka (g).

1006 *Ibid.*, članak 14. stavak 5. točka (b).

1007 Radna skupina iz članka 29., *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. listopada 2017., str. 14.

1008 Opća uredba o zaštiti podataka, članak 19.

Voditelj obrade podataka može zatražiti posebna odstupanja od tih prava i u slučaju obrade osobnih podataka za potrebe arhiviranja u javnom interesu, u svrhe znans-tenog ili povijesnog istraživanja ili u statističke svrhe¹⁰⁰⁹.

U pogledu **izrade profila i automatiziranog donošenja odluka** OUZP-om su uvedena posebna pravila. U članku 22. stavku 1. utvrđuje se da ispitanik „ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, koja proizvodi pravne učinke koji se na njega odnose“. Kako se ističe u smjernicama Radne skupine iz članka 29., tim se člankom utvrđuje opća zabrana potpuno automatiziranog donošenja odluka¹⁰¹⁰. Voditelji obrade podataka mogu biti izuzeti iz takve zabrane samo u trima posebnim slučajevima, ako je odluka: 1) potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade, 2) dopuštena pravom Unije ili države članice, ili 3) utemeljena na izričitoj privoli ispitanika¹⁰¹¹.

Osobna kontrola

Složenost i nedostatak transparentnosti analitike velikih podataka mogli bi zahtijevati promjene poimanja osobne kontrole nad osobnim podacima. Ona bi trebala biti prilagođena danom društvenom i tehnološkom kontekstu, uzimajući u obzir nedostatak informacija pojedinaca. Stoga bi se u zaštiti podataka u vezi s velikim podacima trebao usvojiti širi koncept kontrole nad uporabom podataka, prema kojemu se osobna kontrola razvija u složeniji postupak višestrukih procjena učinaka rizika povezanih s uporabom podataka¹⁰¹².

Koliko je neka aplikacija velikih podataka dobra, ovisi o tome koliko precizno može predvidjeti želje i ponašanje pojedinaca (ili potrošača) koji je testiraju. Postojeći prognostički modeli koji se temelje na analitici velikih podataka neprekidno se usavršavaju. Inovacije uključuju ne samo upotrebu podataka za kategorizaciju tipova osobnosti (odnosno ponašanja i stavova) nego i analizu ponašanja putem analize glasovnih obrazaca i intenziteta pisanja poruka ili tjelesne temperature. Sve se te informacije mogu upotrebljavati u stvarnom vremenu u odnosu na saznanja koja proizlaze iz procjena velikih podataka, primjerice za procjenu kreditne sposobnosti tijekom sastanka s bankarom. Procjena se ne donosi na temelju zasluga osobe koja

1009 *Ibid.*, članak 89. stavci 2. i 3.

1010 Radna skupina iz članka 29., *Smjernice o automatiziranom pojedinačnom donošenju odluka i izradi profila za potrebe Uredbe 2016/679*, WP 251, 3. listopada 2017., str. 9.

1011 Opća uredba o zaštiti podataka, članak 22. stavak 2.

1012 Vijeće Europe, Savjetodavni odbor Konvencije br. 108, *Smjernice o zaštiti pojedinaca u pogledu obrade osobnih podataka u svijetu velikih podataka*, T-PD(2017)01, Strasbourg, 23. siječnja 2017.

podnosi zahtjev za kredit, nego na obilježjima ponašanja koja proizlaze iz analize i procjene velikih podataka, odnosno na temelju govora snažnim ili ugodnim glasom, govora tijela ili tjelesne temperature.

Izrada profila i ciljano oglašavanje ne moraju nužno biti problematični ako su osobe **svjesne** da su podvrgnute posebno prilagođenim oglasima. Izrada profila postaje problem kada se upotrebljava za manipuliranje pojedincima, npr. za traženje određenih tipova osobnosti ili skupina osoba za političke kampanje. Primjerice, skupinama neodlučnih glasača mogu biti upućene političke poruke prilagođene njihovoj osobnosti i stavovima. Drugi je mogući problem upotreba izrade profila za uskraćivanje pristupa određenih pojedinaca proizvodima i uslugama. Jedna zaštitna mjera kojom se može osigurati zaštita od zlorabe velikih podataka i osobnih podataka jest pseudonimizacija (vidjeti [dio 2.1.1.](#))¹⁰¹³. Kada su osobni podaci potpuno anonimizirani, odnosno ne sadrže informacije koje se mogu povezati s ispitanikom, ti slučajevi izlaze iz područja primjene Opće uredbe o zaštiti podataka. Privola ispitanika i pojedinaca u kontekstu obrade velikih podataka također predstavlja izazov za zakonodavstvo o zaštiti podataka. To obuhvaća privolu na primanje prilagođenih oglasa i izradu profila, koji se mogu opravdati razlozima „korisničkog iskustva“, te privolu na uporabu skupova osobnih podataka za usavršavanje i razvoj analitičkih alata koji se temelje na informacijama. Svijest o obradi velikih podataka – ili izostanak te svijesti – dovodi do nekoliko pitanja u vezi sa sredstvima kojima ispitanici mogu ostvariti svoja prava, s obzirom na to da se obrada velikih podataka može temeljiti i na pseudonimiziranim i anonimiziranim podacima koji su podvrgnuti algoritmima. Dok su pseudonimizirani podaci obuhvaćeni Općom uredbom o zaštiti podataka, Uredba se ne primjenjuje na anonimizirane podatke. Osobna kontrola nad obradom vlastitih podataka i svijest o njoj ključne su za analitiku velikih podataka. Bez njih nije moguće sa sigurnošću znati tko je voditelj, a tko izvršitelj obrade podataka, čime se onemogućava učinkovito ostvarivanje osobnih prava.

1013 *Ibid.*, str. 2.

10.2. Tehnologije Web 2.0 i 3.0: društvene mreže i internet stvari

Ključne točke

- Usluge socijalnog umrežavanja (engl. *Social Networking Services*, SNS) mrežne su platforme za komunikaciju koje pojedincima omogućuju da se pridružuju mrežama istomišljenika ili da ih stvaraju.
- Internet stvari (engl. *Internet of Things*) predstavlja povezivanje objekata s internetom te međupovezivanje tih objekata.
- Privola ispitanika najčešća je pravna osnova za zakonitu obradu podataka koju voditelji obrade provode na društvenim mrežama.
- Korisnici društvenih mreža uglavnom su zaštićeni „izuzećem za kućanstvo“, no to se odstupanje može ukinuti u određenim kontekstima.
- Pružatelji usluga društvenih mreža nisu zaštićeni „izuzećem za kućanstvo“.
- Tehnička i integrirana zaštita podataka ključne su za osiguravanje sigurnosti podataka u tom području.

10.2.1. Definiranje tehnologija Web 2.0 i 3.0

Usluge socijalnog umrežavanja

Internet je prvotno bio zamišljen kao mreža za povezivanje računala i prenošenje poruka s ograničenim mogućnostima razmjene podataka, a internetske stranice trebale su pojedincima pružati tek mogućnost pasivnog pregleda njihova sadržaja¹⁰¹⁴. U doba tehnologije Web 2.0 internet je pretvoren u forum u sklopu kojega korisnici mogu komunicirati, surađivati i stvarati sadržaj. Ovo je razdoblje obilježio nevjerojatan uspjeh i raširena upotreba usluga socijalnog umrežavanja, koje su sada neizostavan dio svakodnevnog života milijuna ljudi.

Usluge socijalnog umrežavanja (SNS), ili „društvene mreže“, općenito se mogu definirati kao „mrežne platforme za komunikaciju koje pojedincima omogućuju da se pridružuju mrežama istomišljenika ili ih stvaraju“¹⁰¹⁵. Da bi stvorili mrežu ili joj se

¹⁰¹⁴ Europska komisija (2016.), *Postizanje napretka u pogledu interneta stvari u Europi*, SWD(2016) 110 final.

¹⁰¹⁵ Radna skupina iz članka 29. (2009.), *Mišljenje 5/2009 o društvenim mrežama na internetu*, WP 163, 12. lipnja 2009., str. 4.

pridružili, pojedinci trebaju dostaviti osobne podatke i izraditi profil. SNS omogućuje korisnicima stvaranje digitalnog „sadržaja“, koji obuhvaća fotografije, videozapise, poveznice na novinske članke i osobne objave u kojima izražavaju mišljenje. Putem tih mrežnih platformi za komunikaciju korisnici mogu ostvariti kontakt i komunicirati s nekoliko drugih korisnika. Važna je činjenica da većina popularnih SNS-ova ne zahtijeva nikakve naknade za registraciju. Umjesto obvezivanja korisnika da plate za pridruživanje mreži, pružatelji SNS-ova većinu prihoda ostvaruju od ciljanog oglašavanja. Oglašivači mogu ostvariti veliku korist od osobnih podataka koji se svakodnevno otkrivaju na tim internetskim stranicama. Informacije o dobi, spolu, lokaciji i interesima korisnika omogućuju da njihovi oglasi dopru do „odgovarajućih“ ljudi.

Odbor ministara Vijeća Europe donio je [Preporuku o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja](#) (dostupnu na engleskom jeziku)¹⁰¹⁶, čiji se jedan dio odnosi posebno na zaštitu podataka te je 2018. dopunjen Preporukom o ulogama i odgovornostima internetskih posrednika¹⁰¹⁷.

Primjer: Nora je vrlo sretna jer ju je njezin partner zaprosio. Želi podijeliti tu sretnu vijest s obitelji i prijateljima te odlučuje napisati emotivnu objavu na društvenoj mreži u kojoj izražava svoju radost te mijenja status veze u „zaručena“. Sljedećih nekoliko dana prilikom prijave u račun Nora se prikazuju oglasi o vjenčanicama i cvjećarnicama. Zašto se to događa?

Kada stvaraju oglase na Facebooku, tvrtke koje se bave prodajom vjenčanica i cvijeća odabiru određene parametre kako bi mogle doprijeti do osoba kao što je Nora. Kada Norin profil pokazuje da je ona žena, zaručena i živi u Parizu, u blizini područja u kojima se nalaze saloni vjenčanica i cvjećarnice koje prikazuju oglase, Nori se odmah počinju prikazivati ti oglasi.

Internet stvari

Internet stvari (IoT) predstavlja sljedeći korak u razvoju interneta: razdoblje tehnologije Web 3.0. Uz pomoć IoT-a uređaji se mogu povezati i komunicirati s drugim uređajima putem interneta. To omogućuje da se objekti i osobe međusobno povežu putem komunikacijskih mreža i izvješćuju o svojem statusu i/ili o statusu

¹⁰¹⁶ Vijeće Europe, Odbor ministara, Preporuka CM/Rec(2012)4 Odbora ministara državama članicama o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja, 4. travnja 2012.

¹⁰¹⁷ Vijeće Europe, Odbor ministara, Preporuka CM/Rec(2018)2 Odbora ministara državama članicama o ulogama i odgovornostima internetskih posrednika, 7. ožujka 2018.

okruženja¹⁰¹⁸. IoT i povezani uređaji već su postali stvarnost i očekuje se da će nastaviti znatno rasti u nadolazećim godinama te da će se stvoriti i dodatno razviti pametni uređaji koji će dovesti do stvaranja pametnih gradova, pametnih domova i pametnih poduzeća.

Primjer: IoT može biti posebno koristan za zdravstvo. Tvrtke su već izradile uređaje, senzore i aplikacije koje omogućuju praćenje zdravlja pacijenata. Upotrebom nosivog gumba za alarm i drugih bežičnih senzora koji se postavljaju u domu moguće je pratiti svakodnevne navike starijih osoba koje žive same i slati upozorenja ako dođe do većih promjena njihova dnevnog rasporeda. Primjerice, starije osobe često upotrebljavaju senzore pada. Ti senzori mogu precizno otkriti padove i obavijestiti liječnika i/ili obitelj te osobe o njezinu padu.

Primjer: Barcelona je jedan od najpoznatijih primjera pametnog grada. Grad od 2012. uvodi inovativne tehnologije čiji je cilj stvoriti pametan sustav javnog prijevoza, zbrinjavanja otpada, parkiranja i ulične rasvjete. Primjerice, kako bi se poboljšalo zbrinjavanje otpada, u gradu se upotrebljavaju pametne kante za otpad. One omogućuju praćenje razine otpada radi optimizacije ruta za njegovo prikupljanje. Kada su kante gotovo pune, odašilju signale putem mobilne komunikacijske mreže, koji se šalju softverskoj aplikaciji koju upotrebljava tvrtka za zbrinjavanje otpada. Tvrtka tako može isplanirati najbolju rutu za prikupljanje otpada, određivati prioritete i/ili organizirati preuzimanje samo onih kanti koje se trebaju isprazniti.

10.2.2. Odvagivanje koristi i rizika

Snažno širenje i velik uspjeh SNS-ova u proteklom desetljeću ukazuju na to da oni donose **značajne koristi**. Primjerice, ciljano oglašavanje (opisano u istaknutom primjeru) posebno je inovativan način na koji poduzeća mogu doprijeti do potrošača i prodrijeti na specifično tržište. Također bi moglo biti u interesu potrošača da im se prikazuju oglasi koji su im relevantniji i zanimljiviji. Važno je istaknuti i da usluge socijalnog umrežavanja i društvene mreže mogu imati pozitivan učinak na društvo i uvođenje promjena. One korisnicima omogućuju komunikaciju, interakciju te organiziranje skupina i događaja u vezi s temama koje utječu na njih.

¹⁰¹⁸ Europska komisija, Radni dokument službi Komisije, *Postizanje napretka u pogledu interneta stvari u Europi*, SWD(2016) 110, 19. travnja 2016.

Jednako tako, očekuje se da IoT pruži znatne koristi gospodarstvu pa je dio strategije EU-a za razvoj jedinstvenog digitalnog tržišta. Procjenjuje se da će u EU-u tijekom 2020. broj veza u sklopu IoT-a narasti na šest milijardi. Očekuje se da će širenje povezanosti donijeti važne gospodarske koristi zahvaljujući razvoju inovativnih usluga i aplikacija, boljeg zdravstva, boljeg razumijevanja potreba potrošača i povećane učinkovitosti.

S druge strane, s obzirom na to da korisnici društvenih mreža stvaraju goleme količine osobnih podataka koje zatim operatori usluga obrađuju, uz širenje SNS-ova veže se **sve veća zabrinutost** oko načina na koji se privatnost i osobni podaci mogu zaštititi. SNS-ovi mogu ugroziti pravo na privatni život i pravo na slobodu izražavanja. Mogu se javiti sljedeće prijetnje: „izostanak zakonskih i postupovnih zaštitnih mjera za procese koji mogu dovesti do isključenosti korisnika; neodgovarajuća zaštita djece i mladih od štetnog sadržaja ili ponašanja; manjak poštovanja za prava drugih; manjak zadanih postavki koje omogućuju privatnost; manjak transparentnosti u vezi sa svrhama u koje se osobni podaci prikupljaju i obrađuju”¹⁰¹⁹. Europskim zakonodavstvom o zaštiti podataka nastoji se suprotstaviti izazovima zaštite privatnosti/podataka koje nose društvene mreže. Načela privole, tehničke i integrirane zaštite privatnosti/podataka te prava pojedinaca posebno su važna u kontekstu društvenih mreža i usluga umrežavanja.

U kontekstu IoT-a vrlo velika količina osobnih podataka koji nastaju na različitim međusobno povezanim uređajima također uključuje rizike za privatnost i zaštitu podataka. Iako je transparentnost važno načelo europskog zakonodavstva o zaštiti podataka, zbog velikog broja povezanih uređaja nije uvijek jasno tko može pristupiti podacima prikupljenima s uređaja iz mreže IoT-a te ih prikupljati i upotrebljavati¹⁰²⁰. Međutim, sukladno pravu Unije i Vijeća Europe, načelom transparentnosti uvjetuje se obveza voditelja obrade da jasnim i razumljivim jezikom obavještuje ispitanike o načinu upotrebe njihovih podataka. Rizici, pravila, zaštitne mjere i prava u pogledu obrade njihovih osobnih podataka moraju biti jasni dotičnim pojedincima. Uređaji povezani putem IoT-a te brojni postupci obrade i predmetni podaci također mogu dovesti u pitanje zahtjev davanja jasne privole utemeljene na informacijama za obradu podataka, u slučajevima u kojima je takva obrada utemeljena na privoli. Pojedinci često nedovoljno razumiju tehnički aspekt takve obrade, a stoga i posljedice davanja privole.

¹⁰¹⁹ Vijeće Europe, Preporuka Rec(2012)4 državama članicama o zaštiti ljudskih prava u vezi s uslugama društvenog umrežavanja, 4. travnja 2012.

¹⁰²⁰ Europski nadzornik za zaštitu podataka (2017.), *Understanding the Internet of Things* (Razumijevanje interneta stvari).

Drugo je važno pitanje sigurnost, s obzirom na to da su povezani uređaji posebno izloženi sigurnosnim rizicima. Povezani uređaji imaju različite razine zaštite. Budući da se upotrebljavaju izvan standardne informatičke infrastrukture, mogu im nedostajati odgovarajuća procesorska snaga i kapacitet pohrane koji su potrebni za instaliranje softvera ili primjenu metoda poput šifriranja, pseudonimizacije ili anonimizacije radi zaštite osobnih podataka korisnika.

Primjer: Njemački su zakonodavci odlučili uvesti zabranu igranje koje se povezuje s internetom nakon što je iznesena zabrinutost u vezi s utjecajem igranje na poštovanje privatnog života djece. Zaključili su da je lutka imena Cayla koja se povezuje s internetom, zapravo, prikriveni uređaj za špijuniiranje. Lutka je slala zvučna pitanja koje je dijete postavljalo tijekom igre aplikaciji na digitalnom uređaju, koja ih je pretvarala u tekst i zatim tražila odgovor putem interneta. Aplikacija bi zatim poslala odgovor lutki, koja bi ga izgovorila djetetu. Tom bi se lutkom mogla snimati komunikacija djeteta i odraslih osoba u blizini i slati aplikaciji. Da proizvođači lutke nisu primijenili odgovarajuće sigurnosne mjere, lutku je netko mogao upotrijebiti za prisluškivanje razgovora.

10.2.3. Problemi povezani sa zaštitom podataka

Privola

U Europi je obrada osobnih podataka zakonita samo ako je dopuštena europskim zakonodavstvom o zaštiti podataka. Za pružatelje SNS-ova privola ispitanika uglavnom predstavlja zakonitu osnovu za obradu podataka. Privola mora biti dobrovoljno dana, posebna, utemeljena na informacijama i nedvosmislena (vidjeti [dio 4.1.1.](#))¹⁰²¹. „Dobrovoljno dana” u osnovi znači da ispitanici moraju imati mogućnost stvarnog odabira. Privola je „posebna” i „utemeljena na informacijama” kada je razumljiva i jasno i precizno upućuje na cjelovit opseg, svrhe i posljedice obrade podataka. U kontekstu društvenih mreža može biti upitno je li privola dobrovoljno dana, posebna i utemeljena na informacijama za sve vrste obrade koje provode operator SNS-a i treće strane.

¹⁰²¹ Opća uredba o zaštiti podataka, članci 4. i 7.; modernizirana Konvencija br. 108, članak 5.

Primjer: Za pridruživanje i pristup SNS-u pojedinci često moraju pristati na različite vrste obrade svojih osobnih podataka, i to bez potrebnih konkretnih informacija ili drugih mogućnosti. Primjer je potreba davanja privole za primanje bihevioralnih oglasa radi registracije u SNS. Kako navodi Radna skupina iz članka 29. u svojem Mišljenju o definiciji privole, „s obzirom na važnost koju su neke društvene mreže stekle, određene kategorije korisnika (poput tinejdžera) prihvatit će primanje bihevioralnih oglasa kako bi izbjegle rizik od djelomičnog isključivanja iz društvene interakcije. Korisnik bi trebao biti u poziciji da pruži dobrovoljnu i posebnu privolu za primanje bihevioralnih oglasa, neovisno o njegovu pristupu usluzi socijalnog umrežavanja”¹⁰²².

Prema Općoj uredbi o zaštiti podataka, osobni podaci djece mlađe od 16 godina u načelu se ne smiju obrađivati na temelju njihove privole¹⁰²³. Ako je za obradu potrebna privola, mora je dati roditelj ili skrbnik djeteta. Djeci je potrebna posebna zaštita zbog toga što mogu biti manje svjesna rizika i posljedica obrade podataka. To je vrlo važno u kontekstu društvenih mreža jer su djeca izloženija određenim negativnim učincima koji se mogu javiti prilikom njihove upotrebe, poput virtualnog zlostavljanja (engl. *cyberbullying*), uhođenja putem interneta ili krađe identiteta.

Sigurnost i tehnička i integrirana zaštita privatnosti/podataka

Obrada osobnih podataka nosi određene neizbježne sigurnosne rizike s obzirom na to da postoji neprestana mogućnost povrede sigurnosti koja vodi do nehotičnog ili nezakonitog uništenja, gubitka, izmjene ili otkrivanja obrađenih osobnih podataka ili neovlaštenog pristupa njima. Prema europskom zakonodavstvu o zaštiti podataka, voditelji obrade i izvršitelji obrade obvezni su provesti odgovarajuće tehničke i organizacijske mjere kako bi spriječili neovlašteno ometanje postupaka obrade podataka. Pružatelji usluga socijalnog umrežavanja koji podliježu europskim propisima o zaštiti podataka također moraju poštovati tu obvezu.

Prema načelima tehničke i integrirane zaštite privatnosti/podataka, od voditelja obrade zahtijeva se da održavaju sigurnost tehničke izrade svojih proizvoda i automatski primjenjuju odgovarajuće postavke privatnosti i zaštite podataka. To znači da kada se neka osoba odluči pridružiti društvenoj mreži, pružatelj usluga ne mora

¹⁰²² Radna skupina iz članka 29. (2011.), *Mišljenje 15/2011 o definiciji privole*, WP 187, 13. srpnja 2011., str. 18.

¹⁰²³ Vidjeti Opću uredbu o zaštiti podataka, članak 8. Države članice EU-a mogu zakonom propisati nižu dobnu granicu, pod uvjetom da ona nije niža od 13 godina.

automatski pružiti sve informacije o novom korisniku usluge svim svojim korisnicima. Prilikom priključivanja na uslugu zadane postavke privatnosti i zaštite podataka trebaju biti takve da su informacije dostupne samo odabranim kontaktima te osobe. Omogućivanje pristupa osobama izvan tog popisa trebalo bi biti moguće tek nakon što korisnik ručno promijeni zadane postavke privatnosti i zaštite podataka. To može imati utjecaja i u slučajevima u kojima dođe do povrede podataka unatoč uspostavljenim sigurnosnim mjerama. U takvim slučajevima pružatelji usluga moraju obavijestiti dotične korisnike ako postoji vjerojatnost da će doći do visokog rizika za prava i slobode ispitanika¹⁰²⁴.

Tehnička i integrirana zaštita privatnosti/podataka posebno su važne u kontekstu SNS-ova s obzirom na to da, povrh rizika od neovlaštenog pristupa koje nosi većina vrsta obrade, i dijeljenje osobnih podataka na društvenim mrežama uzrokuje dodatne sigurnosne rizike. Oni su obično uzrokovani nedovoljnim razumijevanjem pojedinaca u pogledu toga *tko* može pristupati njihovim informacijama i kako ih može upotrebljavati. Kako raste raširenost upotrebe društvenih mreža, tako raste i broj incidenata krađe identiteta i njezinih žrtava.

Primjer: Krađa identiteta pojava je do koje dolazi kada jedna osoba dođe do informacija, podataka ili dokumenata koji pripadaju drugoj osobi (žrtvi) i zatim upotrebljava te podatke da bi se lažno predstavljala kao žrtva i dobivala proizvode i usluge u njezino ime. Na primjer, Paul ima korisnički račun na internetskoj stranici jedne društvene mreže. Paul je nastavnik i aktivan član svoje zajednice, vrlo je druželjubiv i nije pretjerano zabrinut oko postavki privatnosti i zaštite podataka na svojem računu za društvenu mrežu. Ima dug popis kontakata, koji ponekad uključuju i osobe koje ne poznaje nužno osobno. Budući da je zaposlen u velikoj školi te je vrlo popularan kao trener školske nogometne momčadi, vjeruje da su ti ljudi najvjerojatnije roditelji ili prijatelji osoba koje rade u školi ili je pohađaju. Paulova adresa e-pošte i datum rođenja vidljivi su na njegovu računu za društvenu mrežu. Osim toga, Paul redovito objavljuje fotografije svojeg psa Tobyja, uz opise poput „Toby i ja u jutarnjoj šetnji”. Paul nije svjestan da je jedno od najpopularnijih sigurnosnih pitanja za zaštitu računa e-pošte ili mobilnog telefona „Kako se zove vaše kućni ljubimac?”. Upotrebom informacija koje su dostupne u Paulovu profilu na društvenoj mreži Nick jednostavno uspijeva hakirati Paulove račune.

1024 *Ibid.*, članak 34.

Prava pojedinaca

Pružatelji SNS-ova moraju poštovati prava pojedinaca (vidjeti [dio 6.1.](#)), uključujući pravo na informacije o svrsi obrade i načinu upotrebe osobnih podataka u svrhe direktnog marketinga. Pojedincima se također mora osigurati pravo na pristup osobnim podacima koje su stvorili u okviru platforme društvene mreže i na zahtjev za njihovo brisanje. Čak i kada osobe pristanu na obradu osobnih podataka i učitaju podatke na mrežu, trebale bi imati mogućnost zatražiti da „budu zaboravljene” ako više ne žele primati usluge te društvene mreže. Pravom na prenosivost podataka korisnicima se dodatno omogućuje primanje kopije osobnih podataka koje pruže pružatelju usluga socijalnog umrežavanja u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te prenošenje vlastitih podataka od jednog pružatelja usluga socijalnog umrežavanja drugome¹⁰²⁵.

Voditelji obrade

Teško pitanje koje se često postavlja u kontekstu društvenih mreža jest tko je voditelj obrade, odnosno tko je osoba koja ima obvezu i odgovornost pridržavanja propisa o zaštiti podataka. Pružatelji usluga socijalnog umrežavanja smatraju se voditeljima obrade sukladno europskom zakonodavstvu o zaštiti podataka. To je vidljivo prema širokoj definiciji pojma „voditelja obrade” te činjenici da ti pružatelji usluga određuju svrhu i sredstva obrade osobnih podataka koje dijele pojedinci. Sukladno pravu EU-a, ako pružaju usluge ispitanicima u EU-u, voditelji obrade moraju se pridržavati odredbi Opće uredbe o zaštiti podataka, čak i ako nemaju nastan u EU-u.

Međutim, mogu li se i korisnici usluga socijalnog umrežavanja smatrati voditeljima obrade? Ako pojedinci obrađuju osobne podatke „tijekom isključivo osobnih ili kućnih aktivnosti”, propisi o zaštiti podataka ne primjenjuju se. To je u europskom zakonodavstvu o zaštiti podataka poznato kao „izuzeće za kućanstvo”. Međutim, u nekim slučajevima korisnik usluge socijalnog umrežavanja možda nije obuhvaćen izuzećem za kućanstvo.

Korisnici dobrovoljno dijele svoje osobne podatke na mreži. Međutim, informacije koje se dijele na mreži često uključuju osobne podatke drugih osoba.

¹⁰²⁵ Opća uredba o zaštiti podataka, članak 21.

Primjer: Paul ima korisnički račun na vrlo popularnoj platformi društvene mreže. Paul pokušava postati glumac i služi se računom da bi objavljivao fotografije, videozapise i objave u kojima objašnjava svoju strast prema umjetnosti. Popularnost je važna za njegovu budućnost, te stoga odlučuje da bi njegov profil trebao biti dostupan ne samo uskom krugu njegovih kontakata nego svim korisnicima interneta, neovisno o tome jesu li članovi mreže. Smije li Paul objavljivati fotografije i videozapise sebe i svoje prijateljice Sarah bez njezine privole? Sarah je učiteljica nižih razreda osnovne škole pa nastoji čuvati svoj privatni život podalje od poslodavca, svojih učenika i njihovih roditelja. Zamislite slučaj u kojemu Sarah, koja se ne služi društvenim mrežama, sazna od zajedničkog prijatelja Nicka da je fotografija nje i Paula na zabavi objavljena na internetu. U takvu slučaju Paulova obrada podataka ne potpada pod pravo Unije jer je obuhvaćena „izuzećem za kućanstvo“.

Međutim, neophodno je da korisnici budu svjesni i imaju na umu da učitanje podataka o drugim osobama bez njihove privole može uzrokovati povredu prava na privatnost i zaštitu podataka tih osoba. Čak i kada se primjenjuje izuzeće za kućanstvo, primjerice ako korisnik ima profil koji je dostupan samo popisu kontakata koje on odabere, taj bi korisnik i dalje mogao snositi odgovornost za objavu osobnih podataka o drugima. Iako se propisi o zaštiti podataka ne primjenjuju ako se primjenjuje izuzeće za kućanstvo, odgovornost može proizlaziti iz primjene drugih nacionalnih propisa, primjerice u slučaju klevete i povrede prava osobnosti. Naposljetku, izuzećem za kućanstvo zaštićeni su samo korisnici SNS-ova: voditelji obrade i izvršitelji obrade koji pružaju sredstva za takvu privatnu obradu obuhvaćeni su zakonodavstvom EU-a o zaštiti podataka¹⁰²⁶.

Nakon reforme Direktive o privatnosti i elektroničkim komunikacijama, propisi o zaštiti podataka, privatnosti i sigurnosti koji se primjenjuju na pružatelje telekomunikacijskih usluga u sklopu postojećeg pravnog okvira primjenjivali bi se i na usluge komunikacije među uređajima i elektroničke komunikacijske usluge, uključujući, primjerice, OTT usluge.

¹⁰²⁶ *Ibid.*, uvodna izjava 18.



Dodatna literatura

Poglavlje 1.

Araceli Mangas, M. (ed.) (2008.), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012.), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Beč, Manz'sche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance”, *International Data Privacy Law*, sv. 6, br. 3, str. 195.–209.

EDRi, *An introduction to data protection*, Bruxelles.

Frowein, J. i Peukert, W. (2009.), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. i Gellert, G. (2012.), „The fundamental right of data protection in the European Union: in search of an uncharted right”, *International Review of Law, Computers and Technology*, sv. 26 (1), str. 73.–82.

Grabenwarter, C. i Pabel, K. (2012.), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poulet, Y., de Hert, P., de Terwangne, C. i Nouwt, S. (Eds.) (2009.), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009.), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016.), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016.), „EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation”.

Jarass, H. (2010.), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. i Sobotta, C. (2013.), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR”, *International Data Privacy Law*, sv. 3, br. 4, str. 222.–228.

Kranenborg, H. (2015.), „Google and the Right to be Forgotten”, *European Data Protection Law Review*, sv. 1, br. 1, str. 70.–79.

Lynskey, O. (2014.), „Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order”, *International and Comparative Law Quarterly*, sv. 63, br. 3, str. 569.–597.

Lynskey, O. (2015.), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Meyer, J. (2011.), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012.), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. i Hofstätter, T. (2012.), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. i Coutron, L. (2010.), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruxelles, Emile Bruylant.

Simitis, S. (1997.), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?“, *Neue Juristische Wochenschrift*, br. 5, str. 281.–288.

Warren, S. i Brandeis, L. (1890.), „The right to privacy“, *Harvard Law Review*, sv. 4, br. 5, str. 193.–220.

White, R. i Ovey, C. (2010.), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Poglavlje 2.

Acquisty, A. i Gross R. (2009.), „Predicting Social Security numbers from public data“, *Proceedings of the National Academy of Science*, 7. srpnja 2009.

Carey, P. (2009.), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. i Blondel V. D. (2013.), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, sv. 3, 2013.

Delgado, L. (2008.), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012.), *La protection des données à caractère personnel*, Pariz, LexisNexis.

Di Martino, A. (2005.), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014.), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. i Boardman, R. (2012.), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010.), „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, sv. 57, br. 6, str. 1701.–1777.

Samarati, P. i Sweeney, L. (1998.), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, tehnično izjvešče SRI-CSL-98-04.

Sweeney, L. (2002.), „K-Anonymity: A Model for Protecting Privacy“ *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, sv. 10, br. 5, str. 557–570.

Tinnefeld, M., Buchner, B. i Petri, T. (2012.), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012.), *Anonymisation: managing data protection risk. Code of practice*.

Poglavlja od 3. do 6.

Brühann, U. (2012.), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ u: Grabitz, E., Hilf, M. i Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008.), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010.), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. i Kaye, J. (2010.), „Revoking consent: a 'blind spot' in data protection law?“, *Computer Law & Security Review*, sv. 26, br. 3, str. 273–283.

Dammann, U. i Simitis, S. (1997.), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. i Papakonstantinou, V. (2012.), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, sv. 22, br. 6, str. 1–5.

De Hert, P. i Papakonstantinou, V. (2012.), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals“, *Computer Law & Security Review*, sv. 28, br. 2, str. 130–142.

Ferretti, F. (2012.), „A European perspective on data processing consent through the re-conceptualization of European data protection’s looking glass after the Lisbon treaty: Taking rights seriously”, *European Review of Private Law*, sv. 20, br. 2, str. 473.–506.

FRA (Agencija Europske unije za temeljna prava) (2010.), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luksemburg, Ured za publikacije Europske unije (Ured za publikacije).

FRA (2010.), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferencijsko izdanje), Beč, FRA.

FRA (2011.), *Access to justice in Europe: an overview of challenges and opportunities*, Luksemburg, Ured za publikacije.

Irish Health Information and Quality Authority (2010.), *Guidance on Privacy Impact Assessment in Health and Social Care*.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. i Saxby, S. (2011.), „30 years on – The review of the Council of Europe Data Protection Convention 108”, *Computer Law & Security Review*, sv. 27, br. 3, str. 223.–231.

Simitis, S. (2011.), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner’s Office, *Privacy Impact Assessment*.

Poglavlje 7.

Europski nadzornik za zaštitu podataka (2014.), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Pouillet, Y., De Hert, P., De Terwangne, C. i Nouwt, S. (2009.), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007.), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013.), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Radna skupina iz članka 29. (2005.), Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

Poglavlje 8.

Blasi Casagran, C. (2016.) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012.), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin, Springer.

De Hert, P. i Papakonstantinou, V. (2012.), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis”, *Computers & Law Magazine of SCL*, sv. 22, br. 6, str. 1.–5.

Drewer, D., Ellermann, J. (2012.), „Europol’s data protection framework as an asset in the fight against cybercrime”, *ERA Forum*, sv. 13, br. 3, str. 381.–395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012.), *Data Protection at Europol*, Luksemburg, Ured za publikacije.

Gutiérrez Zarza, A. (2015.), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Pouillet, Y. i De Hert, P. (2010.), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y., De Hert, P. i Leenes, R. (2011.), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011.), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem”, *European Law Review*, sv. 36, br. 5, str. 722.–776.

Santos Vara, J. (2013.), The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon, Centre for the Law of External Relations, CLEER, radni dokumenti 2013/2.

Poglavlje 9.

Büllesbach, A., Gijrath, S., Poulet, Y. i Hacon, R. (2010.), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. i Poulet, Y. (2012.), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y. i De Hert, P. (2010.), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y., De Hert, P. i Leenes, R. (2011.), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011.), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem”, *European Law Review*, sv. 36, br. 5, str. 722.–776.

Rosemary, J. i Hamilton, A. (2012.), *Data protection law and practice*, London, Sweet & Maxwell.

Poglavlje 10.

El Emam, K. i Álvarez, C. (2015.), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques”, *International Data Privacy Law*, sv. 5, br. 1, str. 73.–87.

Mayer-Schönberger, V. i Cate, F. (2013.), „Notice and consent in a world of Big Data”, *International Data Privacy Law*, sv. 3, br. 2, str. 67.–73.

Rubinstein, I. (2013.), „Big Data: The End of Privacy or a New Beginning?”, *International Data Privacy Law*, sv. 3, br. 2, str. 74.–87.

Sudska praksa

Odabrana sudska praksa Europskog suda za ljudska prava

Pristup osobnim podacima

Gaskin protiv Ujedinjene Kraljevine, br. 10454/83, 7. srpnja 1989.

Godelli protiv Italije, br. 33783/09, 25. rujna 2012.

K. H. i drugi protiv Slovačke, br. 32881/04, 28. travnja 2009.

Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.

M. K. protiv Francuske, br. 19522/09, 18. travnja 2013.

Odièvre protiv Francuske [VV], br. 42326/98, 13. veljače 2003.

Odvagivanje zaštite podataka, slobode izražavanja i prava na informacije

Axel Springer AG protiv Njemačke [VV], br. 39954/08, 7. veljače 2012.

Bohlen protiv Njemačke, br. 53495/09, 19. veljače 2015.

Coudec i Hachette Filipacchi Associés protiv Francuske [VV], br. 40454/07, 10. studenoga 2015.

Magyar Helsinki Bizottság protiv Mađarske [VV], br. 18030/11, 8. studenoga 2016.

Müller i drugi protiv Švicarske, br. 10737/84, 24. svibnja 1988.

Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske [VV], br. 931/13, 27. lipnja 2017.

Vereinigung bildender Künstler protiv Austrije, br. 68354/01, 25. siječnja 2007.

Von Hannover protiv Njemačke (br. 2) [VV], br. 40660/08 i 60641/08, 7. veljače 2012.

Odvagivanje zaštite podataka i slobode vjeroispovijedi

Sinan Işık protiv Turske, br. 21924/05, 2. veljače 2010.

Izazovi mrežne zaštite podataka

K. U. protiv Finske, br. 2872/02, 2. prosinca 2008.

Privola ispitanika

Elberte protiv Latvije, br. 61243/08, 13. siječnja 2015.

Sinan Işık protiv Turske, br. 21924/05, 2. veljače 2010.

Y protiv Turske, br. 648/10, 17. veljače 2015.

Dopisivanje

Amann protiv Švicarske [VV], br. 27798/95, 16. veljače 2000.

Bernh Larsen Holding AS i drugi protiv Norveške, br. 24117/08, 14. ožujka 2013.

Cemalettin Canli protiv Turske, br. 22427/04, 18. studenoga 2008.

D. L. protiv Bugarske, br. 7472/14, 19. svibnja 2016.

Dalea protiv Francuske, br. 964/07, 2. veljače 2010.

Gaskin protiv Ujedinjene Kraljevine, br. 10454/83, 7. srpnja 1989.

Haralambie protiv Rumunjske, br. 21737/03, 27. listopada 2009.

Khelili protiv Švicarske, br. 16188/07, 18. listopada 2011.

Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.

Malone protiv Ujedinjene Kraljevine, br. 8691/79, 2. kolovoza 1984.

Rotaru protiv Rumunjske [VV], br. 28341/95, 4. svibnja 2000.

S. i Marper protiv Ujedinjene Kraljevine [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.

Shimovolos protiv Rusije, br. 30194/09, 21. lipnja 2011.

Silver i drugi protiv Ujedinjene Kraljevine, br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983.

Sunday Times protiv Ujedinjene Kraljevine, br. 6538/74, 26. travnja 1979.

Udruženje za europsku integraciju i ljudska prava i Ekimdzhiev protiv Bugarske, br. 62540/00, 28. lipnja 2007.

Baze podataka o kaznenim evidencijama

Aycaguer protiv Francuske, br. 8806/12, 22. lipnja 2017.

B. B. protiv Francuske, br. 5335/06, 17. prosinca 2009.

Brunet protiv Francuske, br. 21010/10, 18. rujna 2014.

M. K. protiv Francuske, br. 19522/09, 18. travnja 2013.

M. M. protiv Ujedinjene Kraljevine, br. 24029/07, 13. studenoga 2012.

Sigurnost podataka

Haralambie protiv Rumunjske, br. 21737/03, 27. listopada 2009.

K. H. i drugi protiv Slovačke, br. 32881/04, 28. travnja 2009.

Baze podataka o DNK-u

S. i Harper protiv Ujedinjene Kraljevine [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.

Podaci GPS-a

Uzun protiv Njemačke, br. 35623/05, 2. rujna 2010.

Zdravstveni podaci

Avilkina i drugi protiv Rusije, br. 1585/09, 6. lipnja 2013.

Biriuk protiv Litve, br. 23373/03, 25. studenoga 2008.

I. protiv Finske, br. 20511/03, 17. srpnja 2008.

L. H. protiv Latvije, br. 52019/07, 29. travnja 2014.

L. L. protiv Francuske, br. 7508/02, 10. listopada 2006.

M. S. protiv Švedske, br. 20837/92, 27. kolovoza 1997.

Szuluk protiv Ujedinjene Kraljevine, br. 36936/05, 2. lipnja 2009.

Y protiv Turske, br. 648/10, 17. veljače 2015.

Z protiv Finske, br. 22009/93, 25. veljače 1997.

Identitet

Ciubotaru protiv Moldavije, br. 27138/04, 27. travnja 2010.

Godelli protiv Italije, br. 33783/09, 25. rujna 2012.

Odièvre protiv Francuske [VV], br. 42326/98, 13. veljače 2003.

Informacije o profesionalnim djelatnostima

G. S. B. protiv Švicarske, br. 28601/11, 22. prosinca 2015.

M. N. i drugi protiv San Marina, br. 28005/12, 7. srpnja 2015.

Michaud protiv Francuske, br. 12323/11, 6. prosinca 2012.

Niemietz protiv Njemačke, br. 13710/88, 16. prosinca 1992.

Presretanje komunikacije

Amann protiv Švicarske [VV], br. 27798/95, 16. veljače 2000.

Brito Ferrinho Bexiga Villa-Nova protiv Portugala, br. 69436/10, 1. prosinca 2015.

Copland protiv Ujedinjene Kraljevine, br. 62617/00, 3. travnja 2007.

Halford protiv Ujedinjene Kraljevine, br. 20605/92, 25. lipnja 1997.

Iordachi i drugi protiv Moldavije, br. 25198/02, 10. veljače 2009.

Kopp protiv Švicarske, br. 23224/94, 25. ožujka 1998.
Liberty i drugi protiv Ujedinjene Kraljevine, br. 58243/00, 1. srpnja 2008.
Malone protiv Ujedinjene Kraljevine, br. 8691/79, 2. kolovoza 1984.
Mustafa Sezgin Tanrikulu protiv Turske, br. 27473/06, 18. srpnja 2017.
Pruteanu protiv Rumunjske, br. 30181/05, 3. veljače 2015.
Szuluk protiv Ujedinjene Kraljevine, br. 36936/05, 2. lipnja 2009.

Obveze nositelja dužnosti

B. B. protiv Francuske, br. 5335/06, 17. prosinca 2009.
I. protiv Finske, br. 20511/03, 17. srpnja 2008.
Mosley protiv Ujedinjene Kraljevine, br. 48009/08, 10. svibnja 2011.

Osobni podaci

Amann protiv Švicarske [VV], br. 27798/95, 16. veljače 2000.
Bernh Larsen Holding AS i drugi protiv Norveške, br. 24117/08, 14. ožujka 2013.
Uzun protiv Njemačke, br. 35623/05, 2. rujna 2010.

Fotografije

Sciacca protiv Italije, br. 50774/99, 11. siječnja 2005.
Von Hannover protiv Njemačke, br. 59320/00, 24. lipnja 2004.

Pravo na zaborav

Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske [VV], br. 931/13, 27. lipnja 2017.
Segerstedt-Wiberg i drugi protiv Švedske, br. 62332/00, 6. lipnja 2006.

Pravo na prigovor

Leander protiv Švedske, br. 9248/81, 26. ožujka 1987.
M. S. protiv Švedske, br. 20837/92, 27. kolovoza 1997.
Mosley protiv Ujedinjene Kraljevine, br. 48009/08, 10. svibnja 2011.
Rotaru protiv Rumunjske [VV], br. 28341/95, 4. svibnja 2000.
Sinan Işık protiv Turske, br. 21924/05, 2. veljače 2010.

Osjetljive kategorije podataka

Brunet protiv Francuske, br. 21010/10, 18. rujna 2014.
I. protiv Finske, br. 20511/03, 17. srpnja 2008.
Michaud protiv Francuske, br. 12323/11, 6. prosinca 2012.
S. i Marper protiv Ujedinjene Kraljevine [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.

Nadzor i provedba (uloga različitih subjekata, uključujući nadzorna tijela)

I. protiv Finske, br. 20511/03, 17. srpnja 2008.

K. U. protiv Finske, br. 2872/02, 2. prosinca 2008.

Von Hannover protiv Njemačke, br. 59320/00, 24. lipnja 2004.

Von Hannover protiv Njemačke (br. 2) [VV], br. 40660/08 i 60641/08, 7. veljače 2012.

Metode nadzora

Allan protiv Ujedinjene Kraljevine, br. 48539/99, 5. studenoga 2002.

Bărbulescu protiv Rumunjske [VV], br. 61496/08, 5. rujna 2017.

D. L. protiv Bugarske, br. 7472/14, 19. svibnja 2016.

Dragojević protiv Hrvatske, br. 68955/11, 15. siječnja 2015.

Karabeyoğlu protiv Turske, br. 30083/10, 7. lipnja 2016.

Klass i drugi protiv Njemačke, br. 5029/71, 6. rujna 1978.

Roman Zakharov protiv Rusije [VV], br. 47143/06, 4. prosinca 2015.

Rotaru protiv Rumunjske [VV], br. 28341/95, 4. svibnja 2000.

Szabó i Vissy protiv Mađarske, br. 37138/14, 12. siječnja 2016.

Taylor-Sabori protiv Ujedinjene Kraljevine, br. 47114/99, 22. listopada 2002.

Udruženje za europsku integraciju i ljudska prava i Ekimdzhiev protiv Bugarske, br. 62540/00, 28. lipnja 2007.

Uzun protiv Njemačke, br. 35623/05, 2. rujna 2010.

Versini-Campinchi i Crasnianski protiv Francuske, br. 49176/11, 16. lipnja 2016.

Vetter protiv Francuske, br. 59842/00, 31. svibnja 2005.

Vukota-Bojić protiv Švicarske, br. 61838/10, 18. listopada 2016.

Videonadzor

Köpke protiv Njemačke, br. 420/07, 5. listopada 2010.

Peck protiv Ujedinjene Kraljevine, br. 44647/98, 28. siječnja 2003.

Glasovni uzorci

P. G. i J. H. protiv Ujedinjene Kraljevine, br. 44787/98, 25. rujna 2001.

Wisse protiv Francuske, br. 71611/01, 20. prosinca 2005.

Odabrana sudska praksa Suda Europske unije

Sudska praksa koja se odnosi na Direktivu o zaštiti podataka

Spojeni predmeti C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) protiv Administración del Estado*, 24. studenoga 2011.

[Ispravna provedba članka 7. točke (f) Direktive o zaštiti podataka – „zakoniti interesi drugih” – u nacionalnom zakonodavstvu]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) protiv Netlog NV*, 16. veljače 2012.

[Obveza pružatelja usluga društvenih mreža u pogledu sprečavanja nezakonite uporabe glazbenih i audiovizualnih uradaka od strane internetskih korisnika]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija*, 9. ožujka 2017.

[Pravo na brisanje osobnih podataka; pravo na prigovor na obradu]

C-553/07, *College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer*, 7. svibnja 2009.

[Pravo ispitanika na pristup]

C-543/09, *Deutsche Telekom AG protiv Bundesrepublik Deutschland*, 5. svibnja 2011.

[Nužnost obnavljanja privole]

Spojeni predmeti C-293/12 i C-594/12, *Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr.* [VV], 8. travnja 2014.

[Kršenje primarnog prava Unije Direktivom o zadržavanju podataka; zakonita obrada; ograničenje svrhe i pohrane]

C-288/12, *Europska komisija protiv Mađarske* [VV], 8. travnja 2014.

[Zakonitost ukidanja ureda nacionalnog nadzornika za zaštitu podataka]

C-614/10, *Europska komisija protiv Republike Austrije* [VV], 16. listopada 2012.

[Neovisnost nacionalnog nadzornog tijela]

C-518/07, *Europska komisija protiv Savezne Republike Njemačke* [VV], 9. ožujka 2010.

[Neovisnost nacionalnog nadzornog tijela]

C-212/13, *František Ryneš protiv Úřad pro ochranu osobních údajů*, 11. prosinca 2014.

[Pojmovi „obrada podataka“ i „voditelj obrade“]

C-131/12, *Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González* [VV], 13. svibnja 2014.

[Obveze pružatelja internetskih pretraživača da na zahtjev ispitanika ne prikazuju osobne podatke u rezultatima pretrage; primjenjivost Direktive o zaštiti podataka; pojam „obrada podataka“; značenje „voditelja obrade“; uspostavljanje ravnoteže između zaštite podataka i slobode izražavanja; pravo na zaborav]

C-524/06, *Heinz Huber protiv Bundesrepublik Deutschland* [VV], 16. prosinca 2008.

[Zakovitost zadržavanja podataka o strancima u statističkom registru]

C-473/12, *Institut professionnel des agents immobiliers (IPI) protiv Geoffreyja Engleberta i dr.*, 7. studenoga 2013.

[Pravo na obavješćivanje o obradi osobnih podataka]

C-101/01, *Kazneni postupak protiv Bodil Lindqvist*, 6. studenoga 2003.

[Posebne kategorije osobnih podataka]

C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* [VV], 6. listopada 2015.

[Načelo zakonite obrade; temeljna prava; nevaljanost Odluke o „sigurnoj luci“; ovlasti nacionalnih nadzornih tijela]

C-291/12, *Michael Schwarz protiv Stadt Bochum*, 17. listopada 2013.

[Zahtjev za prethodnu odluku; područje slobode, sigurnosti i pravde; biometrijska putovnica; otisci prstiju; pravna osnova; razmjernost]

C-582/14, *Patrick Breyer protiv Bundesrepublik Deutschland*, 19. listopada 2016.

[Pojam „osobni podaci“; adrese internetskog protokola; pohranjivanje koje provodi pružatelj usluga internetskih medija; nacionalni propis koji ne omogućuje da voditelj obrade uzme o obzir postavljeni zakoniti interes]

C-434/16, *Peter Nowak protiv Data Protection Commissioner*, Mišljenje nezavisne odvjetnice Kokott, 20. srpnja 2017.

[Pojam osobnih podataka; pristup vlastitom ispitnom radu; napomene ispravljača]

T-462/12 R, *Pilkington Group Ltd protiv Europske komisije*, Rješenje predsjednika Općeg suda, 11. ožujka 2013.

C-275/06, *Productores de Música de España (Promusicae) protiv Telefónica de España SAU* [VV], 29. siječnja 2008.

[Pojam „osobni podaci”; obveza pružatelja pristupa internetu da otkriju identitet korisnika programa za razmjenu datoteka KaZaA udruženju za zaštitu intelektualnog vlasništva]

Spojeni predmeti C-465/00, C-138/01 i C-139/01, *Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauer mann protiv Österreichischer Rundfunk*, 20. svibnja 2003.

[Proporcionalnost pravne obveze objave osobnih podataka o plaćama zaposlenika određenih kategorija institucija povezanih s javnim sektorom]

C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. studenoga 2011.

[Informacijsko društvo; autorsko pravo; internet; softver za povezivanje ravnopravnih računala; pružatelji internetskih usluga; instalacija sustava za filtriranje elektroničkih komunikacija radi sprečavanja zajedničkog korištenja datoteka kojim se krše autorska prava; nepostojanje opće obveze nadzora prenesenih informacija]

C-201/14, *Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.*, 1. listopada 2015.

[Pravo na obavješćivanje o obradi osobnih podataka]

Spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i dr.* [VV], 21. prosinca 2016.

[Povjerljivost elektroničkih komunikacija; pružatelji elektroničkih komunikacijskih usluga; obveza koja se odnosi na opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji; nepostojanje prethodnog nadzora suda ili nadzora neovisnog upravnog tijela; Povelja Europske unije o temeljnim pravima; usklađenost s pravom Unije]

C-73/07, *Tietosuojavaluutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy* [VV], 16. prosinca 2008.

[Pojam „novinarskih djelatnosti” u smislu članka 9. Direktive o zaštiti podataka]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde protiv Rīgas pašvaldības SIA „Rīgas satiksme”*, 4. svibnja 2017.

[Načelo zakonite obrade: zakonit interes treće strane]

Spojeni predmeti C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen* [VV], 9. studenoga 2010.

[Pojam „osobni podaci”; proporcionalnost pravne obveze objavljivanja osobnih podataka o korisnicima određenih potpora iz poljoprivrednih fondova Europske unije]

C-230/14, *Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. listopada 2015.

[Ovlasti nacionalnih nadzornih tijela]

C-342/12, *Worten – Equipamentos para o Lar, SA protiv Autoridade para as Condições de Trabalho (ACT)*, 30. svibnja 2013.

[Pojam „osobni podaci”; evidencija radnog vremena; načela povezana s kvalitetom podataka i kriterijima za zakonitost obrade podataka; pristup nacionalnog tijela nadležnog za nadzor radnih uvjeta; obveza poslodavca da stavi na raspolaganje evidenciju o radnom vremenu radi izravnog uvida]

Spojeni predmeti C-141/12 i C-372/12, *Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.*, 17. srpnja 2014.

[Opseg prava ispitanika na pristup; zaštita fizičkih osoba u vezi s obradom osobnih podataka; pojam „osobnih podataka”; podaci koji se odnose na podnositelja zahtjeva za dozvolu za boravak i pravna analiza u pripremnom upravnom dokumentu za odluku; Povelja Europske unije o temeljnim pravima]

Sudska praksa koja se odnosi na Direktivu 2016/681

Mišljenje 1/15 Suda [VV], 26. srpnja 2017.

[Pravna osnova; Prijedlog sporazuma između Kanade i Europske unije o prijenosu i obradi podataka iz popisa imena zrakoplovnih putnika; usklađenost Prijedloga sporazuma s člankom 16. UFEU-a i člancima 7. i 8. te člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima]

Sudska praksa koja se odnosi na Uredbu o zaštiti podataka u institucijama Europske unije

C-615/13 P, *ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA) i Europske komisije*, 16. srpnja 2015.
[Pristup dokumentima]

C-28/08 P, *Europska komisija protiv The Bavarian Lager Co. Ltd* [VV], 29. lipnja 2010.
[Pristup dokumentima]

Sudska praksa koja se odnosi na Direktivu 2002/58/EZ

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB protiv Perfect Communication Sweden AB*, 19. travnja 2012.

[Autorsko pravo i srodna prava; obrada podataka putem interneta; kršenje isključivog prava; stavljanje audioknjiga na raspolaganje putem FTP poslužitelja na internetu s IP adrese koju dodjeljuje pružatelj internetskih usluga; sudski nalog izdan pružatelju internetskih usluga kojim se zahtijeva da pruži ime i adresu korisnika IP adrese]

C-70/10, *Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. studenoga 2011.

[Informacijsko društvo; autorsko pravo; internet; softver za povezivanje ravnopravnih računala; pružatelj internetskih usluga; instalacija sustava za filtriranje elektroničkih komunikacija radi sprečavanja zajedničkog korištenja datoteka kojim se krše autorska prava; nepostojanje opće obveze nadzora prenesenih informacija]

C-536/15, *Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)*, 15. ožujka 2017.

[Načelo nediskriminacije; stavljanje na raspolaganje osobnih podataka pretplatnika u svrhu njihove objave u telefonskom imeniku odnosno njihovo korištenje u svrhu javno dostupne usluge davanja obavijesti o brojevima pretplatnika; pretplatnikova privola; razlika ovisno o državi članici u kojoj se pruža javno dostupna usluga davanja obavijesti o brojevima pretplatnika i/ili telefonskih imenika]

Spojeni predmeti C-203/15 i C-698/15, *Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i dr.* [VV], 21. prosinca 2016.

[Povjerljivost elektroničkih komunikacija; pružatelj elektroničkih komunikacijskih usluga; obveza koja se odnosi na opće i neselektivno zadržavanje podataka o prometu i podataka o lokaciji; nepostojanje prethodnog nadzora suda ili nadzora neovisnog upravnog tijela; Povelja Europske unije o temeljnim pravima; usklađenost s pravom Unije]

Kazalo

Sudska praksa Suda Europske unije

<i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECMD) protiv Administración del Estado, spojeni predmeti C-468/10 i C-469/10, 24. studenoga 2011.</i>	32, 55, 142, 144, 159, 160
<i>Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) protiv Netlog NV, C-360/10, 16. veljače 2012.</i>	77
<i>Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB protiv Perfect Communication Sweden AB, C-461/10, 19. travnja 2012.</i>	77
<i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce protiv Salvatorea Mannija, C-398/15, 9. ožujka 2017.</i>	19, 80, 84, 101, 206, 207, 228, 233
<i>ClientEarth i Pesticide Action Network Europe (PAN Europe) protiv Europske agencije za sigurnost hrane (EFSA) i Europske komisije, C-615/13 P, 16. srpnja 2015.</i>	18, 68, 219
<i>College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer, C-553/07, 7. svibnja 2009.</i>	117, 129, 206, 221
<i>Deutsche Telekom AG protiv Bundesrepublik Deutschland, C-543/09, 5. svibnja 2011.</i>	85, 141, 150

<i>Digital Rights Ireland Ltd protiv Minister for Communications, Marine and Natural Resources i dr. i Kärntner Landesregierung i dr. [VV], spojeni predmeti C-293/12 i C-594/12, 8. travnja 2014.....</i>	<i>22, 47, 49, 63, 117, 118, 128, 132, 244, 246, 278, 302, 303, 354</i>
<i>Europska komisija protiv Mađarske [VV], C-288/12, 8. travnja 2014.</i>	<i>189, 195</i>
<i>Europska komisija protiv Republike Austrije [VV], C-614/10, 16. listopada 2012... </i>	<i>189, 194</i>
<i>Europska komisija protiv Savezne Republike Njemačke [VV], C-518/07, 9. ožujka 2010.</i>	<i>189, 194</i>
<i>Europska komisija protiv The Bavarian Lager Co. Ltd. [VV], C-28/08 P, 29. lipnja 2010.....</i>	<i>18, 66, 208, 243</i>
<i>František Ryneš protiv Úřad pro ochranu osobních údajů, C-212/13, 11. prosinca 2014.....</i>	<i>84, 95, 100, 107</i>
<i>Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (AEPD) i Marija Costeje González [VV], C-131/12, 13. svibnja 2014.</i>	<i>18, 19, 58, 79, 84, 102, 108, 206, 226, 227, 232</i>
<i>Heinz Huber protiv Bundesrepublik Deutschland [VV], C-524/06, 16. prosinca 2008.....</i>	<i>141, 144, 155, 156, 331, 347</i>
<i>Institut professionnel des agents immobiliers (IPI) protiv Geoffreyja Engleberta i dr., C-473/12, 7. studenoga 2013.</i>	<i>205, 211</i>
<i>International Transport Workers' Federation i Finnish Seamen's Union protiv Viking Line ABP i OÜ Viking Line Eesti [VV], C-438/05, 11. prosinca 2007.</i>	<i>246</i>
<i>Kazneni postupak protiv Bodil Lindqvist, C-101/01, 6. studenoga 2003.....</i>	<i>84, 99, 102, 106, 107, 172</i>
<i>Kazneni postupak protiv Giuseppe Francesco Gasparini i dr., C-467/04, 28. rujna 2006.....</i>	<i>246</i>
<i>Maximillian Schrems protiv Data Protection Commissioner [VV], C-362/14, 6. listopada 2015.....</i>	<i>46, 189, 191, 192, 197, 208, 242, 244, 253, 258, 259, 260, 264, 266</i>
<i>Michael Schwarz protiv Stadt Bochum, C-291/12, 17. listopada 2013.</i>	<i>51, 53</i>
<i>Mišljenje 1/15 Suda [VV], 26. srpnja 2017.....</i>	<i>45, 271</i>
<i>Pasquale Foglia protiv Mariella Novello (br. 2), C-244/80, 16. prosinca 1981.</i>	<i>246</i>
<i>Patrick Breyer protiv Bundesrepublik Deutschland, C-582/14, 19. listopada 2016.....</i>	<i>83, 94</i>

<i>Peter Nowak protiv Data Protection Commissioner</i> , C-434/16, Mišljenje nezavisne odvetnice Kokott, 20. srpnja 2017.....	84, 206
<i>Pilkington Group Ltd protiv Europske komisije</i> , T-462/12 R, Rješenje predsjednika Općeg suda, 11. ožujka 2013.	70
<i>Productores de Música de España (Promusicae) protiv Telefónica de España SAU</i> [VV], C-275/06, 29. siječnja 2008.	19, 55, 76, 78, 83, 91
<i>Rechnungshof protiv Österreichischer Rundfunk i dr. i Christa Neukomm i Joseph Lauermann protiv Österreichischer Rundfunk</i> , spojeni predmeti C-465/00, C-138/01 i C-139/01, 20. svibnja 2003.....	65, 144
<i>Scarlet Extended SA protiv Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)</i> , C-70/10, 24. studenoga 2011.....	45, 83, 92, 94
<i>Smaranda Bara i dr. protiv Casa Națională de Asigurări de Sănătate i dr.</i> , C-201/14, 1. listopada 2015.....	92, 117, 123, 205, 211, 351
<i>Tele2 (Netherlands) BV i dr. protiv Autoriteit Consument en Markt (ACM)</i> , C-536/15, 15. ožujka 2017.	85, 141, 150, 151
<i>Tele2 Sverige AB protiv Post- och telestyrelsen i Secretary of State for the Home Department protiv Toma Watsona i drugih</i> [VV], spojeni predmeti C-203/15 i C-698/15, 21. prosinca 2016.	49, 63, 278, 303
<i>Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy</i> [VV], C-73/07, 16. prosinca 2008.	18, 56
<i>Volker und Markus Schecke GbR i Hartmut Eifert protiv Land Hessen</i> [VV], spojeni predmeti C-92/09 i C-93/09, 9. studenoga 2010.....	18, 21, 38, 48, 64, 83, 88, 89
<i>Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság</i> , C-230/14, 1. listopada 2015.	197
<i>Worten – Equipamentos para o Lar, SA protiv Autoridade para as Condições de Trabalho (ACT)</i> , C-342/12, 30. svibnja 2013.....	337
<i>Y. S. protiv Minister voor Immigratie, Integratie en Asiel i Minister voor Immigratie, Integratie en Asiel protiv M. i S.</i> , spojeni predmeti C-141/12 i C-372/12, 17. srpnja 2014.....	83, 89, 92, 206, 219
Sudska praksa Europskog suda za ljudska prava	
<i>Allan protiv Ujedinjene Kraljevine</i> , br. 48539/99, 5. studenoga 2002.	277, 282

<i>Amann protiv Švicarske</i> [VV], br. 27798/95, 16. veljače 2000.....	39, 40, 83, 89, 91
<i>Avilkina i drugi protiv Rusije</i> , br. 1585/09, 6. lipnja 2013.	342
<i>Axel Springer AG protiv Njemačke</i> [VV], br. 39954/08, 7. veljače 2012.....	18, 59
<i>Aycaguer protiv Francuske</i> , br. 8806/12, 22. lipnja 2017.....	281
<i>B. B. protiv Francuske</i> , br. 5335/06, 17. prosinca 2009.....	277, 278, 281
<i>Bărbulescu protiv Rumunjske</i> [VV], br. 61496/08, 5. rujna 2017.	90, 339
<i>Bernh Larsen Holding AS i drugi protiv Norveške</i> , br. 24117/08, 14. ožujka 2013.	83, 87
<i>Biriuk protiv Litve</i> , br. 23373/03, 25. studenoga 2008.	62, 208, 342
<i>Bohlen protiv Njemačke</i> , br. 53495/09, 19. veljače 2015.....	18, 61
<i>Brito Ferrinho Bexiga Villa-Nova protiv Portugala</i> , br. 69436/10, 1. prosinca 2015.....	71
<i>Brunet protiv Francuske</i> , br. 21010/10, 18. rujna 2014.....	224
<i>Cemalettin Canli protiv Turske</i> , br. 22427/04, 18. studenoga 2008.....	206, 223
<i>Ciubotaru protiv Moldavije</i> , br. 27138/04, 27. travnja 2010.....	206, 222
<i>Copland protiv Ujedinjene Kraljevine</i> , br. 62617/00, 3. travnja 2007.....	25, 331, 338
<i>Coudec i Hachette Filipacchi Associés protiv Francuske</i> [VV], br. 40454/07, 10. studenoga 2015.....	60
<i>D. L. protiv Bugarske</i> , br. 7472/14, 19. svibnja 2016.	280
<i>Dalea protiv Francuske</i> , br. 964/07, 2. veljače 2010.....	223, 278, 318
<i>Dragojević protiv Hrvatske</i> , br. 68955/11, 15. siječnja 2015.....	280
<i>Elberte protiv Latvije</i> , br. 61243/08, 13. siječnja 2015.....	85
<i>G. S. B. protiv Švicarske</i> , br. 28601/11, 22. prosinca 2015.....	350, 351
<i>Gaskin protiv Ujedinjene Kraljevine</i> , br. 10454/83, 7. srpnja 1989.....	219
<i>Godelli protiv Italije</i> , br. 33783/09, 25. rujna 2012.....	219
<i>Halford protiv Ujedinjene Kraljevine</i> , br. 20605/92, 25. lipnja 1997.....	349
<i>Haralambie protiv Rumunjske</i> , br. 21737/03, 27. listopada 2009.....	117, 122
<i>I. protiv Finske</i> , br. 20511/03, 17. srpnja 2008.....	26, 142, 170, 341
<i>Iordachi i drugi protiv Moldavije</i> , br. 25198/02, 10. veljače 2009.....	39
<i>K. H. i drugi protiv Slovačke</i> , br. 32881/04, 28. travnja 2009.	117, 120, 219, 341
<i>K. U. protiv Finske</i> , br. 2872/02, 2. prosinca 2008.....	26, 208, 247

<i>Karabeyoğlu protiv Turske</i> , br. 30083/10, 7. lipnja 2016.....	241, 285
<i>Khelili protiv Švicarske</i> , br. 16188/07, 18. listopada 2011.....	42
<i>Klass i drugi protiv Njemačke</i> , br. 5029/71, 6. rujna 1978.....	25, 26, 277, 279
<i>Köpke protiv Njemačke</i> , br. 420/07, 5. listopada 2010.....	95, 247
<i>Kopp protiv Švicarske</i> , br. 23224/94, 25. ožujka 1998.....	39
<i>L. H. protiv Latvije</i> , br. 52019/07, 29. travnja 2014.....	342
<i>L. L. protiv Francuske</i> , br. 7508/02, 10. listopada 2006.....	341
<i>Leander protiv Švedske</i> , br. 9248/81, 26. ožujka 1987.....	42, 44, 206, 219, 232, 281
<i>Liberty i drugi protiv Ujedinjene Kraljevine</i> , br. 58243/00, 1. srpnja 2008.....	87
<i>M. K. protiv Francuske</i> , br. 19522/09, 18. travnja 2013.....	224, 281
<i>M. M. protiv Ujedinjene Kraljevine</i> , br. 24029/07, 13. studenoga 2012.....	131, 281
<i>M. N. i drugi protiv San Marina</i> , br. 28005/12, 7. srpnja 2015.....	92, 350
<i>M. S. protiv Švedske</i> , br. 20837/92, 27. kolovoza 1997.....	232, 341
<i>Magyar Helsinki Bizottság protiv Mađarske</i> [VV], br. 18030/11, 8. studenoga 2016.....	18, 69
<i>Malone protiv Ujedinjene Kraljevine</i> , br. 8691/79, 2. kolovoza 1984.....	25, 40, 277
<i>Michaud protiv Francuske</i> , br. 12323/11, 6. prosinca 2012.....	332, 349
<i>Mosley protiv Ujedinjene Kraljevine</i> , br. 48009/08, 10. svibnja 2011.....	18, 61, 232
<i>Müller i drugi protiv Švicarske</i> , br. 10737/84, 24. svibnja 1988.....	75
<i>Mustafa Sezgin Tanrikulu protiv Turske</i> , br. 27473/06, 18. srpnja 2017.....	25, 241
<i>Niemietz protiv Njemačke</i> , br. 13710/88, 16. prosinca 1992.....	89, 349
<i>Odièvre protiv Francuske</i> [VV], br. 42326/98, 13. veljače 2003.....	219
<i>P. G. i J. H. protiv Ujedinjene Kraljevine</i> , br. 44787/98, 25. rujna 2001.....	95
<i>Peck protiv Ujedinjene Kraljevine</i> , br. 44647/98, 28. siječnja 2003.....	41, 95
<i>Pruteanu protiv Rumunjske</i> , br. 30181/05, 3. veljače 2015.....	18, 71
<i>Roman Zakharov protiv Rusije</i> [VV], br. 47143/06, 4. prosinca 2015.....	26, 283
<i>Rotaru protiv Rumunjske</i> [VV], br. 28341/95, 4. svibnja 2000.....	25, 40, 89, 223, 279
<i>S. i Harper protiv Ujedinjene Kraljevine</i> [VV], br. 30562/04 i 30566/04, 4. prosinca 2008.....	18, 39, 43, 118, 131, 277, 278, 281

<i>Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske</i> [VV], br. 931/13, 27. lipnja 2017.....	20, 57
<i>Sciacca protiv Italije</i> , br. 50774/99, 11. siječnja 2005.	95
<i>Segerstedt-Wiberg i drugi protiv Švedske</i> , br. 62332/00, 6. lipnja 2006.	206, 224
<i>Shimovolos protiv Rusije</i> , br. 30194/09, 21. lipnja 2011.....	40
<i>Silver i drugi protiv Ujedinjene Kraljevine</i> , br. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. ožujka 1983.	40
<i>Sinan Işık protiv Turske</i> , br. 21924/05, 2. veljače 2010.....	73
<i>Sunday Times protiv Ujedinjene Kraljevine</i> , br. 6538/74, 26. travnja 1979.....	40
<i>Szabó i Vissy protiv Mađarske</i> , br. 37138/14, 12. siječnja 2016.....	25, 26, 277, 279, 283
<i>Szuluk protiv Ujedinjene Kraljevine</i> , br. 36936/05, 2. lipnja 2009.....	341
<i>Taylor-Sabori protiv Ujedinjene Kraljevine</i> , br. 47114/99, 22. listopada 2002.	40
<i>Udruženje za europsku integraciju i ljudska prava i Ekimdzhev protiv Bugarske</i> , br. 62540/00, 28. lipnja 2007.	40
<i>Uzun protiv Njemačke</i> , br. 35623/05, 2. rujna 2010.	26, 83
<i>Vereinigung bildender Künstler protiv Austrije</i> , br. 68354/01, 25. siječnja 2007.....	19, 75
<i>Versini-Campinchi i Crasnianski protiv Francuske</i> , br. 49176/11, 16. lipnja 2016.	284
<i>Vetter protiv Francuske</i> , br. 59842/00, 31. svibnja 2005.	40, 277
<i>Von Hannover protiv Njemačke</i> , br. 59320/00, 24. lipnja 2004.....	95
<i>Von Hannover protiv Njemačke (br. 2)</i> [VV], br. 40660/08 i 60641/08, 7. veljače 2012.	55
<i>Vukota-Bojić protiv Švicarske</i> , br. 61838/10, 18. listopada 2016.....	41
<i>Wisse protiv Francuske</i> , br. 71611/01, 20. prosinca 2005.	95
<i>Y protiv Turske</i> , br. 648/10, 17. veljače 2015.	142, 161
<i>Z protiv Finske</i> , br. 22009/93, 25. veljače 1997.	27, 331, 341
Sudska praksa nacionalnih sudova	
Češka Republika, Ustavni sud (<i>Ústavní soud České republiky</i>), 94/2011 Coll., 22. ožujka 2011.	302

Njemačka, Savezni ustavni sud (<i>Bundesverfassungsgericht</i>), 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (<i>Volkszählungsurteil</i>), 15. prosinca 1983.	20
Njemačka, Savezni ustavni sud (<i>Bundesverfassungsgericht</i>), 1 BvR 256/08, 2. ožujka 2010.	302
Rumunjska, Savezni ustavni sud (<i>Curtea Constituțională a României</i>), br. 1258, 8. listopada 2009.	302

Mnoštvo informacija o Agenciji Europske unije za temeljna prava dostupno je na internetu. Može im se pristupiti putem internetskih stranica FRA-a na fra.europa.eu

Dodatne informacije o sudskoj praksi Europskog suda za ljudska prava dostupne su na internetskim stranicama Suda: echr.coe.int. Portal za pretraživanje HUDOC pruža pristup presudama i odlukama na engleskom i/ili francuskom jeziku, prijevode na druge jezike, pravne sažetke, priopćenja za medije i druge informacije o radu Suda (<http://hudoc.echr.coe.int>).

Kako doći do publikacija Vijeća Europe

Council of Europe Publishing izdaje djela u svim područjima rada Organizacije, uključujući ljudska prava, pravne znanosti, zdravstvo, etičnost, društvena pitanja, okoliš, obrazovanje, kulturu, sport, mlade i arhitektonsko nasljeđe. Knjige i elektroničke publikacije iz opsežnog kataloga mogu se naručiti putem interneta (<http://book.coe.int/>).

Virtualna čitaonica korisnicima omogućuje da besplatno prouče isječke iz glavnih radova koji su upravo objavljeni ili cjelovite tekstove određenih službenih dokumenata.

Informacije o konvencijama Vijeća Europe i njihovi cjeloviti tekstovi dostupni su na internetskim stranicama Ureda za ugovore: <http://conventions.coe.int/>

Kontakt s EU-om

Osobno

U cijeloj Europskoj uniji postoje stotine informacijskih centara *Europe Direct*. Adresu najbližeg centra možete pronaći na: https://europa.eu/european-union/contact_hr

Telefonom ili e-poštom

Europe Direct je služba koja odgovara na vaša pitanja o Europskoj uniji. Možete im se obratiti:

- na besplatni telefonski broj: 00 800 6 7 8 9 10 11 (neki operateri naplaćuju te pozive),
- na broj: +32 22999696 ili
- e-poštom preko: https://europa.eu/european-union/contact_hr

Traženje informacija o EU-u

Na internetu

Informacije o Europskoj uniji na svim službenim jezicima EU-a dostupne su na internetskim stranicama Europa: https://europa.eu/european-union/index_hr

Publikacije EU-a

Besplatne publikacije EU-a i publikacije EU-a koje se plaćaju možete preuzeti ili naručiti preko EU Bookshopa: <https://publications.europa.eu/hr/publications>. Za više primjeraka besplatnih publikacija obratite se službi *Europe Direct* ili najbližemu informacijskom centru (vidjeti https://europa.eu/european-union/contact_hr).

Zakonodavstvo EU-a i povezani dokumenti

Za pristup pravnim informacijama iz EU-a, uključujući cjelokupno zakonodavstvo EU-a od 1951. na svim službenim jezičnim verzijama, posjetite internetske stranice EUR-Lexa: <http://eur-lex.europa.eu>

Otvoreni podatci iz EU-a

Portal otvorenih podataka EU-a (<http://data.europa.eu/euodp/hr>) omogućuje pristup podatkovnim zbirkama iz EU-a. Podatci se mogu besplatno preuzimati i ponovno uporabiti u komercijalne i nekomercijalne svrhe.

Brz razvoj informacijske tehnologije povećao je potrebu za snažnom zaštitom osobnih podataka. To je pravo zaštićeno instrumentima i Europske unije (EU) i Vijeća Europe. Zaštita tog važnog prava podrazumijeva nove i značajne izazove dok tehnološki napredak dovodi do pomicanja granica područja poput nadzora, presretanja komunikacija i pohrane podataka. Ovaj je priručnik namijenjen pravnicima koji nisu specijalizirani u području zaštite podataka kako bi se upoznali s ovim novim područjem prava. Priručnik sadržava pregled primjenjivih pravnih okvira Europske unije i Vijeća Europe. U njemu se također objašnjava ključna sudska praksa i sažimaju najvažnije presude Suda Europske unije i Europskog suda za ljudska prava. Usto, u priručniku su predstavljeni hipotetski scenariji koji služe kao praktične ilustracije različitih problema koji se javljaju u ovom području, koje se neprekidno razvija.

FRA – AGENCIJA EUROPSKE UNIJE ZA TEMELJNA PRAVA

Schwarzenbergplatz 11 – 1040 Beč – Austrija

Tel. +43 158030-0 – Faks +43 158030-699

fra.europa.eufacebook.com/fundamentalrightslinkedin.com/company/eu-fundamental-rights-agencytwitter.com/EURightsAgency**EUROPSKI SUD ZA LJUDSKA PRAVA****VIJEĆE EUROPE**

67075 Strasbourg Cedex – Francuska

Tel. +33 (0) 3 88 41 20 18 – Faks +33 (0) 3 88 41 27 30

echr.coe.int – publishing@echr.coe.int**EUROPSKI NADZORNIK ZA ZAŠTITU PODATAKA**

Rue Wiertz 60 – 1047 Brisel – Belgija

Tel. +32 2 283 19 00

edps.europa.eu – edps@edps.europa.eu – @EU_EDPSUred za publikacije
Europske unijeISBN 978-92-871-9835-8 (Vijeće Europe)
ISBN 978-92-9474-442-5 (FRA)