

PRÍRUČKA

Príručka o európskych právnych predpisoch v oblasti ochrany údajov

vydanie 2018



Rukopis tejto príručky bol dokončený v apríli 2018.

V budúcnosti budú k dispozícii aktualizácie príručky na webovej stránke FRA na adrese: fra.europa.eu, na webovej stránke Rady Európy na adrese: coe.int/dataprotection, na webovej stránke Európskeho súdu pre ľudské práva v ponuke Case-Law (Judikatúra) na adrese: echr.coe.int a na webovej stránke Európskeho dozorného úradníka pre ochranu údajov na adrese: edps.europa.eu.

Fotografia na obálke a vo vnútri: © iStockphoto

© Agentúra Európskej únie pre základné práva a Rada Európy, 2021

Reprodukcia je povolená len s uvedením zdroja.

Na akékoľvek použitie alebo reprodukciu fotografií alebo iného materiálu, ktorý nie je predmetom autorského práva Agentúry Európskej únie pre základné práva/Rady Európy, je potrebné povolenie priamo od držiteľov práv. Agentúra Európskej únie pre základné práva/Rada Európy ani iná osoba, ktorá koná v mene Agentúry Európskej únie pre základné práva/Rady Európy nenesie zodpovednosť za prípadné použitie informácií obsiahnutých v tejto publikácii.

Viac doplňujúcich informácií o Európskej únii je k dispozícii na internete (<http://europa.eu>).

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021

Rada Európy:	ISBN 978-92-871-9823-5		
FRA – Print:	ISBN 978-92-9461-308-0	doi:10.2811/836850	TK-05-17-225-SK-C
FRA – PDF:	ISBN 978-92-9461-307-3	doi:10.2811/4464	TK-05-17-225-SK-N

Táto príručka bola vypracovaná v angličtine. Rada Európy a Európsky súd pre ľudské práva (ESLP) nenesú žiadnu zodpovednosť za kvalitu prekladov do iných jazykov. Stanoviská vyjadrené v tejto príručke nie sú pre Radu Európy a ESLP záväzné. V príručke sa odkazuje na vybrané komentáre a príručky. Rada Európy a ESLP nenesú žiadnu zodpovednosť za obsah týchto publikácií a z ich zaradenia do tohto zoznamu v žiadnom prípade nevyplyva ich schválenie. Ďalšie publikácie sú uvedené na internetových stránkach knižnice ESLP na adrese echr.coe.int.

Obsah tejto príručky nepredstavuje oficiálne stanovisko Európskeho dozorného úradníka pre ochranu údajov (EDPS) a nie je pre EDPS záväzný pri výkone jeho právomocí. EDPS nenesie žiadnu zodpovednosť za kvalitu prekladov do iných jazykov ako angličtiny.



Príručka o európskych právnych predpisoch v oblasti ochrany údajov

vydanie 2018

Predslov

Naše spoločnosti sa čoraz viac digitalizujú. V kontexte týchto zmien nás každodenne ovplyvňuje rôznymi spôsobmi tempo technologického rozvoja a spôsob, akým sa spracúvajú osobné údaje. Právne rámce Európskej únie (EÚ) a Rady Európy, ktorým sa zabezpečuje ochrana súkromia a osobných údajov, boli nedávno novelizované.

Európa celosvetovo zohráva vedúcu úlohu v oblasti ochrany údajov. Štandardy EÚ v oblasti ochrany údajov vychádzajú z Dohovoru Rady Európy č. 108, nástrojov EÚ vrátane všeobecného nariadenia o ochrane údajov a smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, ako aj príslušnej judikatúry Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie.

EÚ a Rada Európy vykonávajú v oblasti ochrany údajov rozsiahle reformy, ktoré sú často zložité, a voči jednotlivcom a podnikom sa prejavujú širokou škálou výhod a vplyvov. Cieľom tejto príručky je zvýšiť informovanosť a zlepšiť poznatky o právnych predpisoch v oblasti ochrany údajov, najmä medzi nešpecializovanými právnikmi pôsobiacimi v oblasti práva, ktorí sa s otázkami ochrany údajov stretávajú v rámci svojej práce.

Príručku vypracovala Agentúra EÚ pre základné práva (FRA) spolu s Radou Európy (spolu s kanceláriou Európskeho súdu pre ľudské práva) a Európskym dozorným úradníkom pre ochranu údajov. Ide o aktualizáciu vydania z roku 2014 a je súčasťou série právnych príručiek, ktoré spoločne vypracovali FRA a Rada Európy.

Radi by sme sa poďakovali orgánom pre ochranu osobných údajov z Belgicka, Estónska, Francúzska, Gruzínska, Maďarska, Írska, Talianska, Monaka, Švajčiarska a Spojeného kráľovstva za užitočnú spätnú väzbu k návrhu príručky. Takisto by sme radi vyjadrili vďaka Európskej komisii, oddeleniu pre ochranu údajov a jej oddeleniu pre medzinárodné toky údajov a ochranu údajov. Ďakujeme Súdnemu dvoru Európskej únie za dokumentačnú podporu počas prípravných prác na tejto príručke.

Na záver by sme chceli poďakovať Úradu na ochranu osobných údajov Slovenskej republiky za podporu pri revízii slovenskej verzie tejto príručky.

Christos Giakoumopoulos

generálny riaditeľ pre
ľudské práva a právny štát
Rady Európy

Giovanni Buttarelli

Európsky dozorný
úradník pre ochranu
údajov

Michael O'Flaherty

riaditeľ Agentúry
Európskej únie pre
základné práva

Obsah

PREDSLOV	3
SKRATKY A ACRONYMY	11
AKO POUŽÍVAŤ TÚTO PRÍRUČKU	13
1 KONTEXT A VÝCHODISKÁ EURÓPSKEHO PRÁVA V OBLASTI OCHRANY ÚDAJOV	17
1.1. Právo na ochranu osobných údajov	19
Hlavné body	19
1.1.1. Právo na rešpektovanie súkromného života a právo na ochranu osobných údajov: stručný úvod	20
1.1.2. Medzinárodný právny rámec: Organizácia Spojených národov	24
1.1.3. Európsky dohovor o ľudských právach	25
1.1.4. Dohovor Rady Európy č. 108	26
1.1.5. Právne predpisy Európskej únie o ochrane údajov	29
1.2. Obmedzenia práva na ochranu osobných údajov	38
Hlavné body	38
1.2.1. Požiadavky na oprávnený zásah podľa ECHR	39
1.2.2. Podmienky zákonných obmedzení podľa Charty základných práv EÚ	45
1.3. Vzájomné pôsobenie vo vzťahu k iným právam a oprávneným záujmom	55
Hlavné body	55
1.3.1. Sloboda prejavu	56
1.3.2. Služobné tajomstvo	71
1.3.3. Sloboda náboženského vyznania a viery	74
1.3.4. Sloboda umenia a vedeckého bádania	76
1.3.5. Ochrana duševného vlastníctva	77
1.3.6. Ochrana údajov a hospodárske záujmy	80
2 TERMINOLÓGIA V OBLASTI OCHRANY ÚDAJOV	85
2.1. Osobné údaje	87
Hlavné body	87
2.1.1. Hlavné aspekty pojmu osobný údaj	88
2.1.2. Osobitné kategórie osobných údajov	101

2.2.	Spracúvanie údajov	102
Hlavné body		102
2.2.1.	Koncepcia spracúvania údajov	102
2.2.2.	Automatizované spracúvanie údajov	104
2.2.3.	Neautomatizované spracúvanie údajov	105
2.3.	Používatelia osobných údajov	106
Hlavné body		106
2.3.1.	Prevádzkovatelia a sprostredkovatelia	106
2.3.2.	Príjemcovia a tretie strany	116
2.4.	Súhlas	117
Hlavné body		117
3	HLAVNÉ ZÁSADY EURÓPSKEHO PRÁVA V OBLASTI OCHRANY ÚDAJOV	121
3.1.	Zásady zákonnosti, spravodlivosti a transparentnosti spracúvania	123
Hlavné body		123
3.1.1.	Zákonnosť spracúvania	124
3.1.2.	Spravodlivosť spracúvania	124
3.1.3.	Transparentnosť spracúvania	126
3.2.	Zásada obmedzenia účelu	128
Hlavné body		128
3.3.	Zásada minimalizácie údajov	132
Hlavné body		132
3.4.	Zásada správnosti údajov	134
Hlavné body		134
3.5.	Zásada minimalizácie uchovávaní	135
Hlavné body		135
3.6.	Zásada bezpečnosti údajov	137
Hlavné body		137
3.7.	Zásada zodpovednosti	141
Hlavné body		141
4	PRAVIDLÁ EURÓPSKÝCH PRÁVNÝCH PREDPISOV O OCHRANE ÚDAJOV	145
4.1.	Pravidlá zákonného spracúvania	147
Hlavné body		147
4.1.1.	Právne základy spracúvania údajov	148
4.1.2.	Spracúvanie osobitných kategórií údajov (citlivých údajov)	165

4.2.	Pravidlá bezpečnosti spracúvania	171
	Hlavné body	171
4.2.1.	Prvky bezpečnosti údajov	172
4.2.2.	Dôvernosť	176
4.2.3.	Oznámenia o porušeníach ochrany osobných údajov	178
4.3.	Pravidlá týkajúce sa zodpovednosti a podpory súladu	181
	Hlavné body	181
4.3.1.	Zodpovedné osoby	182
4.3.2.	Záznamy o spracovateľských činnostiach	185
4.3.3.	Posúdenie vplyvu na ochranu údajov a predchádzajúca konzultácia	187
4.3.4.	Kódexy správania	189
4.3.5.	Certifikácia	191
4.4.	Špecificky navrhnutá a štandardná ochrana údajov	191
5	NEZÁVISLÝ DOHLAD	195
	Hlavné body	196
5.1.	Nezávislosť	199
5.2.	Príslušnosť a právomoci	202
5.3.	Spolupráca	206
5.4.	Európsky výbor pre ochranu údajov	208
5.5.	Mechanizmus konzistentnosti podľa GDPR	209
6	PRÁVA DOTKNUTÝCH OSÔB A ICH PRESADZOVANIE	211
6.1.	Práva dotknutých osôb	214
	Hlavné body	214
6.1.1.	Právo byť informovaný	215
6.1.2.	Právo na opravu	228
6.1.3.	Právo na vymazanie („právo na zabudnutie“)	229
6.1.4.	Právo na obmedzenie spracúvania	235
6.1.5.	Právo na prenosnosť údajov	236
6.1.6.	Právo namietať	238
6.1.7.	Automatizované individuálne rozhodovanie vrátane profilovania	242
6.2.	Prostriedky nápravy, zodpovednosť, sankcie a náhrada škody	245
	Hlavné body	245
6.2.1.	Právo podať sťažnosť dozornému orgánu	246
6.2.2.	Právo na účinný súdny prostriedok nápravy	247
6.2.3.	Zodpovednosť a právo na náhradu škody	254
6.2.4.	Sankcie	256

7	MEDZINÁRODNÉ PRENOSY A TOKY OSOBNÝCH ÚDAJOV	259
7.1.	Povaha prenosov osobných údajov	260
	Hlavné body	260
7.2.	Voľný pohyb/tok osobných údajov medzi členskými štátmi alebo zmluvnými stranami	261
	Hlavné body	261
7.3.	Prenosy osobných údajov do tretích krajín/krajín, ktoré nie sú stranami Dohovoru, alebo medzinárodným organizáciám	263
	Hlavné body	263
7.3.1.	Prenosy na základe rozhodnutia o primeranosti	264
7.3.2.	Prenosy vyžadujúce si primerané záruky	268
7.3.3.	Výnimky pre osobitné situácie	273
7.3.4.	Prenosy na základe medzinárodných dohôd	276
8	OCHRANA ÚDAJOV V KONTEXTE POLÍCIE A TRESTNÉHO SÚDNICTVA	281
8.1.	Právne predpisy RE o ochrane údajov a o otázkach národnej bezpečnosti, polície a trestného súdnictva	283
	Hlavné body	283
8.1.1.	Odporúčanie v oblasti polície	285
8.1.2.	Budapešťiansky dohovor o počítačovej kriminalite	290
8.2.	Právne predpisy EÚ o ochrane údajov v oblasti polície a trestného súdnictva	291
	Hlavné body	291
8.2.1.	Smernica o ochrane údajov pre orgány polície a trestného súdnictva	292
8.3.	Iné osobitné právne nástroje týkajúce sa ochrany údajov v oblasti presadzovania práva	301
8.3.1.	Ochrana údajov v súdnych orgánoch a orgánoch presadzovania práva EÚ	311
8.3.2.	Ochrana údajov v spoločných informačných systémoch na úrovni EÚ	318
9	OSOBITNÉ DRUHY ÚDAJOV A PRÍSLUŠNÉ PRAVIDLÁ OCHRANY ÚDAJOV	337
9.1.	Elektronické komunikácie	338
	Hlavné body	338
9.2.	Údaje o zamestnaní	342
	Hlavné body	342
9.3.	Údaje týkajúce sa zdravia	347
	Hlavný bod	347
9.4.	Spracúvanie údajov na výskumné a štatistické účely	352
	Hlavné body	352
9.5.	Finančné údaje	356
	Hlavné body	356

10 MODERNÉ VÝZVY V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV	361
10.1. Big data, algoritmy a umelá inteligencia	363
Hlavné body	363
10.1.1. Vymedzenie big data, algoritmov a umelej inteligencie	364
10.1.2. Vyvažovanie prínosov a rizík big data	366
10.1.3. Otázky súvisiace s ochranou údajov	369
10.2. Web 2.0 a web 3.0: sociálne siete a internet vecí	375
Hlavné body	375
10.2.1. Vymedzenie pojmu web 2.0 a web 3.0	375
10.2.2. Vyvažovanie výhod a rizík	377
10.2.3. Otázky súvisiace s ochranou údajov	379
ODPORÚČANÁ LITERATÚRA	385
JUDIKATÚRA	393
Vybraná judikatúra Európskeho súdu pre ľudské práva	393
Vybraná judikatúra Súdneho dvora Európskej únie	398
INDEX	403

Skratky a akronymy

BCR	záväzné vnútropodnikové pravidlo
CCTV	priemyselná televízia
CETS	Séria zmlúv Rady Európy
CIS	Colný informačný systém
CRM	riadenie vzťahov so zákazníkmi
C-SIS	Centrálny Schengenský informačný systém
Dohovor č. 108	Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Rada Európy) Pozmeňujúci protokol (CETS č. 223) k Dohovoru č. 108 („modernizovaný Dohovor č. 108“) prijal Výbor ministrov Rady Európy pri príležitosti svojho 128. zasadnutia, ktoré sa konalo v meste Elsinore v Dánsku (17. – 18. mája 2018). Odkazy na „modernizovaný Dohovor č. 108“ sa vzťahujú na dohovor zmenený protokolom CETS č. 223.
DPA	orgán pre ochranu osobných údajov
DPO	zodpovedná osoba
ECHR	Európsky dohovor o ľudských právach
EDPB	Európsky výbor pre ochranu údajov
EDPS	Európsky dozorný úradník pre ochranu údajov
EFSA	Európsky úrad pre bezpečnosť potravín
EHS	Európsky hospodársky priestor
ENISA	Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť
EPPO	Európska prokuratúra
ES	Európske spoločenstvo
ESLP	Európsky súd pre ľudské práva
ESMA	Európsky orgán pre cenné papiere a trhy
eTEN	Transeurópske telekomunikačné siete
EÚ	Európska únia
eu-LISA	Agentúra Európskej únie na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti

EuroPriSe	Európske osvedčenie o zachovaní dôverného charakteru informácií
EZR	európsky zatykač
EZVO	Európske združenie voľného obchodu
FRA	Agentúra Európskej únie pre základné práva
GDPR	všeobecné nariadenie o ochrane údajov
GPS	globálny polohový systém
Charta	Charta základných práv Európskej únie
ICCPR	Medzinárodný pakt o občianskych a politických právach
IKT	informačné a komunikačné technológie
ISP	poskytovateľ internetových služieb
MVO	mimovládna organizácia
N.SIS	Národný Schengenský informačný systém
NÚE	Národná ústredňa Europolu
OECD	Organizácia pre hospodársku spoluprácu a rozvoj
OSN	Organizácia Spojených národov
PIN	osobné identifikačné číslo
PNR	záznamy o cestujúcich
RE	Rada Európy
SCG	koordináčna skupina pre dohľad
SDEÚ	Súdny dvor Európskej únie (do decembra 2009 Súdny dvor Európskych spoločenstiev, SDES)
SDO	spoločný dozorný orgán
SEPA	jednotná oblasť platieb v eurách
SIS	Schengenský informačný systém
SWIFT	Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu
Ú. v.	Úradný vestník
UDHR	Všeobecná deklarácia ľudských práv
VIS	vízový informačný systém
ZEÚ	Zmluva o Európskej únii
ZFEÚ	Zmluva o fungovaní Európskej únie

Ako používať túto príručku

V tejto príručke sa uvádzajú právne normy týkajúce sa ochrany údajov, ktoré stanovila Európska únia (EÚ) a Rada Európy. Jej úlohou je pomôcť odborníkom pôsobiacim v oblasti práva, ktorí sa nešpecializujú na oblasť ochrany údajov, vrátane právnikov, sudcov alebo iných odborníkov, ako aj osobám pracujúcim pre iné subjekty, ako sú napríklad mimovládne organizácie (MVO), ktoré sa môžu stretávať s právnymi otázkami z oblasti ochrany údajov.

Táto príručka predstavuje prvý referenčný zdroj, pokiaľ ide o relevantné právo EÚ a Európsky dohovor o ľudských právach (ECHR), ako aj Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor č. 108) a ďalšie nástroje Rady Európy.

V úvode každej kapitoly sa nachádza tabuľka s právnymi ustanoveniami relevantnými pre otázky, ktorým sa daná kapitola venuje. Tabuľky zahŕňajú právo Rady Európy, ako aj právo EÚ a obsahujú vybranú judikatúru Európskeho súdu pre ľudské práva (ESLP) a Súdneho dvora Európskej únie (SDEÚ). Následne sú predstavené príslušné právne predpisy oboch európskych právnych poriadkov, ktoré by sa mohli vzťahovať na jednotlivé otázky. Čitatelia sa tak môžu oboznámiť so spoločnými aj s odlišnými miestami oboch právnych systémov. Ide aj o pomôcku pri hľadaní kľúčových informácií týkajúcich sa konkrétnej situácie, najmä ak sa vzťahuje len právo Rady Európy. V niektorých kapitolách sa poradie tém v tabuľkách môže nepatrne líšiť od štruktúry textu v kapitole, ak je to vhodnejšie z hľadiska stručného predstavenia obsahu kapitoly. V príručke sa tiež uvádza stručný prehľad o príslušnom rámci Organizácie Spojených národov.

Odborníci v štátoch mimo EÚ, ktoré sú členmi Rady Európy a zmluvnými stranami ECHR a Dohovoru č. 108, nájdu informácie relevantné pre ich krajinu tak, že priamo prejdú na oddiely týkajúce sa Rady Európy. Odborníci v štátoch mimo EÚ musia mať na pamäti, že od prijatia všeobecného nariadenia EÚ o ochrane údajov sa pravidlá EÚ na ochranu údajov uplatňujú na organizácie a iné subjekty, ktoré nie sú usadené v EÚ, ak spracúvajú osobné údaje a ponúkajú tovar a služby dotknutým osobám v Únii alebo monitorujú správanie takýchto dotknutých osôb.

Odborníci pôsobiaci v oblasti práva v členských štátoch EÚ budú musieť používať oba oddiely, keďže tieto štáty sú viazané oboma právnymi poriadkami. Je potrebné uviesť, že reformy a modernizácia pravidiel ochrany údajov v Európe, ku ktorým došlo v rámci Rady Európy (modernizovaný Dohovor č. 108 zmenený protokolom

CETS č. 223) a EÚ [prijatie všeobecného nariadenia o ochrane údajov a smernice (EÚ) 2016/680], prebehli paralelne. Normotvorcovia v rámci oboch právnych systémov vynaložili maximálne úsilie na zabezpečenie konzistentnosti a kompatibility medzi týmito dvoma právnymi rámcami. Výsledkom týchto reforiem je tak väčšia miera harmonizácie medzi právnymi predpismi RE a EÚ v oblasti ochrany údajov. Čitatelia, ktorí potrebujú viac informácií o konkrétnom probléme, nájdu v oddiele príručky s názvom *Odporúčaná literatúra* uvedený zoznam odbornejších materiálov. Informácie týkajúce sa ustanovení Dohovoru č. 108 a jeho dodatkového protokolu z roku 2001, ktoré sa uplatňujú až do nadobudnutia platnosti pozmeňujúceho protokolu, nájdu čitatelia vo vydaní príručky z roku 2014.

Právne predpisy RE sú predstavené vo forme krátkych odkazov na vybrané prípady ESĽP. Tieto prípady boli vybrané z veľkého množstva rozsudkov a rozhodnutí, ktoré ESĽP prijal v oblasti ochrany údajov.

Príslušné právne predpisy EÚ zahŕňajú prijaté legislatívne opatrenia, príslušné ustanovenia zmlúv a Charty základných práv Európskej únie tak, ako sa vykladajú v judikatúre SDEÚ. Príručka okrem toho obsahuje stanoviská a usmernenia, ktoré prijala pracovná skupina zriadená podľa článku 29, ako poradný orgán, ktorého úlohou v súlade so smernicou o ochrane údajov je poskytovať odborné poradenstvo členským štátom EÚ, a ktorú od 25. mája 2018 nahradí Európsky výbor pre ochranu údajov (EDPB). Stanoviská Európskeho dozorného úradníka pre ochranu údajov takisto poskytujú dôležité informácie o výklade práva EÚ, a preto sú zahrnuté v tejto príručke.

V judikatúre opísanej alebo citovanej v tejto príručke sa uvádzajú príklady z dôležitého korpusu judikatúry ESĽP aj SDEÚ. Usmernenia uvedené v závere príručky majú pomôcť čitateľom pri vyhľadávaní judikatúry on-line. Uvedená judikatúra SDEÚ sa týka predchádzajúcej smernice o ochrane údajov. Výklad SDEÚ sa však naďalej uplatňuje na zodpovedajúce práva a povinnosti stanovené vo všeobecnom nariadení o ochrane údajov.

Okrem toho sú v textových poliach s modrým pozadím uvedené praktické názorné príklady vo forme hypotetických scenárov. Tieto podrobnejšie ilustrujú uplatňovanie európskych predpisov o ochrane údajov v praxi, a to najmä v prípadoch, keď k danej téme neexistuje žiadna špecifická judikatúra ESĽP alebo SDEÚ. V textových poliach so sivým pozadím sú uvedené príklady z iných zdrojov, než je judikatúra ESĽP a SDEÚ, ako sú napríklad právne predpisy a stanoviská vydané pracovnou skupinou zriadenou podľa článku 29.

Príručka sa začína stručným opisom úlohy dvoch právnych systémov stanovených ECHR a právnymi predpismi EÚ ([Kapitola 1](#)). Kapitoly 2 až 8 sa týkajú nasledujúcich tém:

- terminológia v oblasti ochrany údajov,
- hlavné zásady európskych právnych predpisov o ochrane údajov,
- pravidlá európskych právnych predpisov o ochrane údajov,
- nezávislý dohľad,
- práva dotknutých osôb a ich presadzovanie,
- cezhraničné prenosy a toky osobných údajov,
- ochrana údajov v kontexte polície a trestného súdnictva,
- ďalšie európske predpisy o ochrane údajov v konkrétnych oblastiach,
- moderné výzvy v oblasti ochrany osobných údajov.

1

Kontext a východiská európskeho práva v oblasti ochrany údajov

EÚ	Zahrnuté témy	RE
Právo na ochranu údajov		
Zmluva o fungovaní Európskej únie, článok 16		ECHR, článok 8 (právo na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie)
Charta základných práv Európskej únie (Charta), článok 8 (právo na ochranu osobných údajov)		Modernizovaný Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (modernizovaný Dohovor č. 108)
Smernica 95/46/EHS o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (smernica o ochrane údajov), Ú. v. ES L 281, 1995 (účinná do mája 2018)		
Rámcové rozhodnutie Rady 2008/977/SVV o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach, Ú. v. EÚ L 350, 2008 (účinné do mája 2018)		
Nariadenie (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), Ú. v. EÚ L 119, 2016		

EÚ	Zahrnuté témy	RE
Smernica (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (ochrana údajov políciou a orgánmi trestného súdnictva), Ú. v. EÚ L 119, 2016 Smernica 2002/58/ES týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 2002 Nariadenie (ES) č. 45/2001 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov (nariadenie o ochrane údajov inštitúciami EÚ), Ú. v. ES L 8, 2001		
Obmedzenia práva na ochranu osobných údajov		
Charta, článok 52 ods. 1 Všeobecné nariadenie o ochrane údajov, článok 23 SDEÚ, spojené veci C-92/09 a C-93/09, <i>Volker und Markus Schecke GbR a Hartmut Eifert/ Land Hessen</i> [VK], 2010		ECHR, článok 8 ods. 2 Modernizovaný Dohovor č. 108, článok 11 ESLP, <i>S. a Marper/ Spojené kráľovstvo</i> [VK], č. 30562/04 a č. 30566/04, 2008
Vyváženie práv		
SDEÚ, spojené veci C-92/09 a C-93/09, <i>Volker und Markus Schecke GbR a Hartmut Eifert/ Land Hessen</i> [VK], 2010	Všeobecne	
SDEÚ, C-73/07, <i>Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy a Satamedia Oy</i> [VK], 2008 SDEÚ, C-131/12, <i>Google Spain SL a Google Inc./ Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [VK], 2014	Sloboda prejavu	ESLP, <i>Axel Springer AG/Nemecko</i> [VK], č. 39954/08, 2012 ESLP, <i>Mosley/ Spojené kráľovstvo</i>, č. 48009/08, 2011 ESLP, <i>Bohlen/Nemecko</i>, č. 53495/09, 2015
SDEÚ, C-28/08 P, <i>Európska komisia/The Bavarian Lager Co. Ltd</i> [VK], 2010 SDEÚ, C-615/13P, <i>ClientEarth, PAN Europe/ EFSA</i>, 2015.	Prístup k dokumentom	ESLP, <i>Magyar Helsinki Bizottság/Maďarsko</i> [VK], č. 18030/11, 2016

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, článok 90	Služobné tajomstvo	ESLP, <i>Pruteanu/Rumunsko</i> , č. 30181/05, 2015
Všeobecné nariadenie o ochrane údajov, článok 91	Sloboda náboženského vyznania a viery	
	Sloboda umenia a vedeckého bádania	ESLP, <i>Vereinigung bildender Künstler/Rakúsko</i> , č. 68354/01, 2007
SDEÚ, C-275/06, <i>Productores de Música de España (Promusicae)/Telefónica de España SAU</i> [VK], 2008	Ochrana vlastníctva	
SDEÚ, C-131/12, <i>Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD)</i> , Mario Costeja González [VK], 2014 SDEÚ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni</i> , 2017	Hospodárske práva	

1.1. Právo na ochranu osobných údajov

Hlavné body

- Podľa článku 8 ECHR je právo osoby na ochranu v súvislosti so spracúvaním osobných údajov súčasťou práva na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie.
- Dohovor Rady Európy č. 108 je prvým a doteraz jediným medzinárodným právne záväzným nástrojom, ktorý sa zaoberá ochranou údajov. Dohovor prešiel procesom modernizácie, ktorá bola dokončená prijatím pozměňujúceho Protokolu CETS č. 223.
- V rámci právnych predpisov EÚ bola ochrana údajov uznaná ako samostatné základné právo. Je zakotvené v článku 16 Zmluvy o fungovaní EÚ, ako aj v článku 8 Charty základných práv EÚ.
- V rámci právnych predpisov EÚ bola ochrana údajov prvýkrát upravená smernicou o ochrane údajov v roku 1995.
- Vzhľadom na rýchly technologický vývoj prijala EÚ v roku 2016 nové právne predpisy s cieľom prispôsobiť pravidlá ochrany údajov digitálnemu veku. Všeobecné nariadenie o ochrane údajov sa začalo uplatňovať v máji 2018, čím sa zrušila smernica o ochrane údajov.

- Spolu so všeobecným nariadením o ochrane údajov prijala EÚ právne predpisy o spracúvaní osobných údajov štátnymi orgánmi na účely presadzovania práva. V smernici (EÚ) 2016/680 sa stanovujú pravidlá a zásady ochrany údajov, ktorými sa upravuje spracúvanie osobných údajov na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania a stíhania alebo na účely výkonu trestných sankcií.

1.1.1. Právo na rešpektovanie súkromného života a právo na ochranu osobných údajov: stručný úvod

Právo na rešpektovanie súkromného života a právo na ochranu osobných údajov, hoci úzko súvisia, sú samostatnými právami. Právo na súkromie – v európskom práve sa naň odkazuje ako na právo na rešpektovanie súkromného života – bolo v medzinárodnom práve v oblasti ľudských práv zakotvené vo Všeobecnej deklarácii ľudských práv (UDHR), ktorá bola prijatá v roku 1948, ako jedno zo základných chránených ľudských práv. Čoskoro po prijatí UDHR Európa takisto potvrdila toto právo – v Európskom dohovore o ľudských právach (ECHR), ktorý pre jeho zmluvné strany predstavuje právne záväznú zmluvu a ktorý bol vypracovaný v roku 1950. V ECHR sa stanovuje, že každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie. Zasahovanie orgánu verejnej moci do tohto práva je zakázané, s výnimkou prípadov, keď je zásah v súlade s právnymi predpismi, sleduje dôležité a legitímne verejné záujmy a je nevyhnutný v demokratickej spoločnosti.

UDHR a ECHR boli prijaté pred začiatkom rozvoja počítačov a internetu a pred rozmachom informačnej spoločnosti. Tento vývoj priniesol jednotlivcom a spoločnosti značné výhody, zlepšila sa kvalita života, zvýšila efektívnosť a produktivita. Zároveň však predstavuje nové riziká pre právo na rešpektovanie súkromného života. V reakcii na potrebu osobitných pravidiel upravujúcich získavanie a používanie osobných informácií vznikla nová koncepcia ochrany súkromia, ktorá sa v niektorých jurisdikciách označuje ako „informačné súkromie“ a v iných ako „právo na informačné sebaurčenie“¹. Táto koncepcia viedla k vypracovaniu osobitných právnych predpisov, ktoré poskytujú ochranu osobných údajov.

1 Spolkový ústavný súd Nemecka potvrdil právo na informačné sebaurčenie v roku 1983 v rozsudku vo veci *Volkszählungsurteil* BVerfGE Bd. 65, s. 1 a nasl. Súd dospel k záveru, že informačné sebaurčenie vyplývajú zo základného práva na rešpektovanie osobnosti, ktoré je chránené v nemeckej ústave. ESLP uznal v rozsudku z roku 2017, že v článku 8 ECHR „sa stanovuje právo na určitú formu informačného sebaurčenia“. Pozri ESLP, *Satakunnan Markkinapörssi Oy a Satamedia Oy /Fínsko*, č. 931/13, 27. júna 2017, bod 137.

Ochrana údajov v Európe sa začala v 70. rokoch minulého storočia tým, že v niektorých štátoch sa prijali právne predpisy na kontrolu spracúvania osobných informácií orgánmi verejnej moci a veľkými spoločnosťami². Nástroje na ochranu údajov boli následne zakotvené na európskej úrovni³ a v priebehu rokov ochrana údajov nadobudla samostatnú hodnotu, ktorá nie je zahrnutá do práva na rešpektovanie súkromného života. V právnom poriadku EÚ sa ochrana údajov uznáva ako základné právo, oddelené od základného práva na rešpektovanie súkromného života. Týmto oddelením vzniká otázka vzťahu a rozdielov medzi týmito dvoma právami.

Právo na rešpektovanie súkromného života a právo na ochranu osobných údajov spolu úzko súvisia. Cieľom oboch týchto práv je chrániť podobné hodnoty, t. j. nezávislosť a ľudskú dôstojnosť jednotlivcov, tým, že im poskytnú osobný priestor, v rámci ktorého môžu slobodne rozvíjať svoje osobnosti, rozmýšľať a formovať svoje názory. Sú teda nevyhnutným predpokladom na uplatňovanie iných základných slobôd, ako sú sloboda prejavu, sloboda pokojného zhromažďovania a združovania a sloboda náboženského vyznania.

Tieto dve práva sa líšia svojou formuláciou a rozsahom pôsobnosti. Právo na rešpektovanie súkromného života pozostáva zo všeobecného zákazu zasahovania, s výnimkou určitých kritérií verejného záujmu, ktoré môžu v určitých prípadoch odôvodňovať zásah. Ochrana osobných údajov sa vníma ako moderné a aktívne právo⁴, ktorým sa zavádza systém brzd a protiváh na ochranu jednotlivcov vždy, keď sa spracúvajú ich osobné údaje. Spracúvanie musí byť v súlade so základnými prvkami ochrany osobných údajov, konkrétne nezávislým dohľadom a rešpektovaním práv dotknutej osoby⁵.

2 Spolková krajina Hesensko prijala v roku 1970 prvý zákon o ochrane údajov, ktorý sa uplatňoval len v tejto spolkovej krajine. V roku 1973 Švédsko prijalo prvý celoštátny zákon o ochrane údajov na svete. Do konca 80. rokov minulého storočia viaceré európske štáty (Francúzsko, Nemecko, Holandsko a Spojené kráľovstvo) takisto prijali právne predpisy o ochrane údajov.

3 Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor č. 108) bol prijatý v roku 1981. EÚ prijala prvý komplexný nástroj na ochranu údajov v roku 1995: smernicu 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.

4 Generálna advokátka Sharpston konštatovala, že v tejto veci ide o dve samostatné práva: „klasické“ právo na ochranu súkromia a „modernejšie“ právo na ochranu osobných údajov. Pozri SDEÚ, spojené veci C-92/09 a C-93/02, *Volker und Markus Schecke GbR/Land Hessen, návrhy, ktoré predniesla generálna advokátka Sharpston*, 17. júna 2010, bod 71.

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, júl 2013.

Článok 8 Charty základných práv EÚ (Charta) nielen potvrdzuje právo na ochranu osobných údajov, ale uvádza aj základné hodnoty spojené s týmto právom. Stanovuje sa v ňom, že pri spracúvaní osobných údajov musí ísť o riadne spracúvanie na určené účely buď na základe súhlasu dotknutej osoby, alebo na inom legitímnom základe ustanovenom zákonom. Jednotlivci musia mať právo na prístup k svojim osobným údajom a právo na ich opravu a dodržiavanie tohto práva musí podliehať kontrole nezávislého orgánu.

Právo na ochranu osobných údajov sa uplatňuje vždy, keď sa spracúvajú osobné údaje, je preto širšie ako právo na rešpektovanie súkromného života. Každá spracovateľská operácia osobných údajov podlieha primeranej ochrane. Ochrana údajov sa týka všetkých druhov osobných údajov a spracúvania údajov bez ohľadu na vzťah so súkromím a vplyv na súkromie. Spracúvaním osobných údajov sa môže tiež porušovať právo na súkromný život, ako sa uvádza v príkladoch uvedených ďalej. Uplatňovanie pravidiel ochrany údajov si však nevyžaduje preukázanie narušenia súkromného života.

Právo na súkromie sa týka situácií, v ktorých bol ohrozený súkromný záujem alebo „súkromný život“ jednotlivca. Ako sa uvádza v tejto príručke, pojem „súkromný život“ sa v judikatúre vo všeobecnosti vykladá tak, že sa vzťahuje na intímne situácie, citlivé alebo dôverné informácie, ktoré by mohli mať vplyv na to, ako jednotlivca vníma verejnosť, a dokonca na aspekty profesionálneho života a správania na verejnosti. Posúdenie existencie alebo neexistencie zásahu do „súkromného života“ však závisí od kontextu a skutkových okolností každého prípadu.

Naopak, akákoľvek operácia zahŕňajúca spracúvanie osobných údajov môže patriť do rozsahu pôsobnosti pravidiel ochrany údajov a viesť k uplatneniu práva na ochranu osobných údajov. Napríklad, ak zamestnávateľ zaznamená informácie o menách zamestnancov a odmenách, ktoré im vyplatil, samotné zaznamenanie týchto informácií nemožno považovať za zásah do súkromného života. Proti takému zásahu by sa však mohlo namietat, ak by napríklad zamestnávateľ preniesol osobné informácie zamestnancov tretím osobám. Zamestnávatelia musia v každom prípade dodržiavať pravidlá ochrany údajov, pretože zaznamenávanie údajov zamestnancov predstavuje spracúvanie údajov.

Príklad: Vo veci *Digital Rights Ireland*⁶ mal SDEÚ rozhodnúť o platnosti smernice 2006/24/ES vzhľadom na základné práva na ochranu osobných údajov a rešpektovanie súkromného života, ktoré sú zakotvené v Charte základných práv EÚ. V smernici sa od poskytovateľov verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí vyžadovalo, aby uchovávali telekomunikačné údaje občanov počas obdobia do dvoch rokov s cieľom zabezpečiť, aby boli tieto údaje k dispozícii na účely prevencie, vyšetrovania a stíhania závažných trestných činov. Toto opatrenie sa vzťahovalo len na metaúdaje, lokalizačné údaje a údaje potrebné na identifikáciu účastníka alebo používateľa. Nevzťahovalo sa na obsah elektronických komunikácií.

SDEÚ považoval smernicu za zásah do základného práva na ochranu osobných údajov, „pretože stanovuje spracovávanie osobných údajov“⁷. Okrem toho konštatoval, že smernica zasahuje do práva na rešpektovanie súkromného života⁸. Zo všetkých týchto osobných údajov uchovaných podľa smernice, ku ktorým by mohli mať prístup príslušné orgány, možno vyvodiť „presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú“⁹. Zásah do týchto dvoch práv bolo rozsiahly a mimoriadne závažný.

SDEÚ vyhlásil smernicu 2006/24/ES za neplatnú, pričom konštatoval, že napriek tomu, že sledovala legitímny cieľ, zásah do práv na ochranu osobných údajov a súkromného života bol závažný a neobmedzoval sa na to, čo je nevyhnutne potrebné.

6 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

7 Tamže, bod 36.

8 Tamže, body 32 – 35.

9 Tamže, bod 27.

1.1.2. Medzinárodný právny rámec: Organizácia Spojených národov

V rámci Organizácie Spojených národov sa ochrana osobných údajov neuznáva ako základné právo, hoci právo na súkromie je v medzinárodnom právnom poriadku ako základné právo zakotvené už dlho. V článku 12 UDHR o rešpektovaní súkromného a rodinného života¹⁰ sa v medzinárodnom nástroji po prvýkrát stanovilo právo jednotlivca na ochranu súkromnej sféry proti zasahovaniu iných osôb, najmä zo strany štátu. Hoci UDHR predstavuje nezáväzné vyhlásenie, má významné postavenie ako základný nástroj medzinárodného práva v oblasti ľudských práv a mala vplyv na vývoj ďalších nástrojov v oblasti ľudských práv v Európe. Medzinárodný pakt o občianskych a politických právach (ICCPR) nadobudol platnosť v roku 1976. Tvrdí sa v ňom, že nikto nesmie byť vystavený svojvoľnému alebo nezákonnému zasahovaniu do súkromia, obydlia alebo korešpondencie ani nezákonným útokom na svoju česť a povesť. ICCPR je medzinárodná zmluva, ktorou sa jej 169 zmluvných strán zaväzujú rešpektovať a zabezpečovať vykonávanie občianskych práv jednotlivcov, vrátane ich súkromia.

Od roku 2013 prijala Organizácia Spojených národov dve rezolúcie o otázkach ochrany súkromia s názvom „právo na súkromie v digitálnom veku“¹¹ v reakcii na vývoj nových technológií a odhalenia týkajúce sa hromadného sledovania vykonávaného v niektorých štátoch (Snowdenove odhalenia). Dôrazne sa v nich odsudzuje hromadné sledovanie a zdôrazňuje sa vplyv takéhoto sledovania na základné práva na súkromie a slobodu prejavu a na fungovanie dynamickej a demokratickej spoločnosti. Napriek tomu, že tieto rezolúcie nie sú právne záväzné, viedli k dôležitej medzinárodnej politickej diskusii na vysokej úrovni o súkromí, nových technológiách a sledovaní. Viedli aj k vytvoreniu pozície osobitného spravodajcu pre právo na súkromie, s mandátom na presadzovanie a ochranu tohto práva. K osobitným úlohám tohto spravodajcu patrí zhromažďovanie informácií o vnútroštátnych postupoch a skúsenostiach v súvislosti so súkromím a výzvami vyplývajúcimi z nových technológií, výmena a podporovanie najlepších postupov a identifikácia potenciálnych prekážok.

Kým predchádzajúce rezolúcie boli zamerané na negatívne účinky hromadného sledovania a zodpovednosť štátov pri obmedzovaní právomoci spravodajských

10 Organizácia spojených národov (OSN), *Všeobecná deklarácia ľudských práv (UDHR)*, 10. decembra 1948.

11 Pozri Valné zhromaždenie OSN, *Rezolúcia o práve na súkromie v digitálnom veku*, A/RES/68/167, New York, 18. decembra 2013; a Valné zhromaždenie OSN, *revidované znenie Rezolúcie o práve na súkromie v digitálnom veku*, A/C.3/69/L.26/Rev.1, New York, 19. novembra 2014.

orgánov, v novších rezolúciách sa odráža zásadný posun diskusie o súkromí v Organizácii Spojených národov¹². V rezolúciách prijatých v rokoch 2016 a 2017 sa opätovne potvrdzuje potreba obmedziť právomoci spravodajských agentúr a odsudzuje hromadné sledovanie. Zároveň sa v nich však výslovne uvádza, že „zvyšujúce sa schopnosti podnikov získavať, spracúvať a využívať osobné údaje môžu predstavovať riziko pre uplatňovanie práva na súkromie v digitálnom veku“. Okrem zodpovednosti štátnych orgánov sa preto v týchto rezolúciách poukazuje na zodpovednosť súkromného sektora za rešpektovanie ľudských práv a spoločnosti sa vyzývajú, aby informovali používateľov o získavaní, používaní, výmene a uchovávaní osobných údajov a aby zaviedli transparentné postupy ich spracúvania.

1.1.3. Európsky dohovor o ľudských právach

Rada Európy vznikla po druhej svetovej vojne s úmyslom spojiť európske štáty pri presadzovaní právneho štátu, demokracie, ľudských práv a spoločenského rozvoja. S týmto cieľom v roku 1950 schválila ECHR, ktorý nadobudol účinnosť v roku 1953.

Zmluvné strany majú medzinárodnú povinnosť dodržiavať ustanovenia ECHR. Vo všetkých členských štátoch RE je ECHR začlenený alebo priamo účinný v ich vnútroštátnych právnych predpisoch, a preto musia konať v zhode s ustanoveniami tohto Dohovoru. Zmluvné strany musia pri výkone každej činnosti alebo právomoci rešpektovať práva stanovené v tomto Dohovore. Platí to aj pre činnosti vykonávané v oblasti národnej bezpečnosti. Prelomové rozsudky Európskeho súdu pre ľudské práva (ESLP) sa týkali pôsobenia štátu v citlivých oblastiach práva a praxe v oblasti národnej bezpečnosti¹³. ESLP bez váhania potvrdil, že činnosti v oblasti sledovania predstavujú zásah do rešpektovania súkromného života¹⁴.

S cieľom zabezpečiť, aby si zmluvné strany plnili povinnosti vyplývajúce z ECHR, bol v Štrasburgu vo Francúzsku v roku 1959 zriadený ESLP. Úlohou ESLP je zabezpečiť, aby štáty plnili záväzky vyplývajúce z Dohovoru a zaoberali sa sťažnosťami jednotlivých osôb, skupín jednotlivcov, mimovládnych organizácií alebo právnických osôb, ktoré sa sťažujú na údajné porušenia Dohovoru. ESLP sa môže zaoberať aj

12 Valné zhromaždenie OSN revidované znenie Rezolúcie o práve na súkromie v digitálnom veku, A/C.3/71/L.39/Rev.1, New York, 16. novembra 2016; Rada OSN pre ľudské práva, Právo na súkromie v digitálnom veku, A/HRC/34/L.7/Rev.1, 22. marca 2017.

13 Pozri napríklad: ESLP, *Klass a i./Nemecko*, č. 5029/71, 6. septembra 1978; ESLP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000 a ESLP, *Szabó a Vissy/Maďarsko*, č. 37138/14, 12. januára 2016.

14 Tamže.

medzištátnymi spormi vedenými jedným členským štátom alebo viacerými členskými štátmi RE proti inému členskému štátu.

V roku 2018 mala Rada Európy 47 zmluvných strán, pričom 28 z nich bolo zároveň členskými štátmi EÚ. Sťažovateľ, ktorý sa obracia na ESĽP, nemusí byť štátnym príslušníkom zmluvnej strany, no k údajným porušeniam muselo dôjsť v jurisdikcii jednej zo zmluvných strán.

Právo na ochranu osobných údajov tvorí časť práv chránených podľa článku 8 ECHR, ktorým sa zaručuje právo na rešpektovanie súkromného a rodinného života, obydla a korešpondencie a stanovujú podmienky prípustnosti obmedzenia tohto práva¹⁵.

ESĽP posudzoval veľa prípadov, ktoré sa týkali ochrany údajov. Okrem iného išlo o prípady odpočúvania komunikácie¹⁶, rôznych foriem sledovania zo strany súkromného aj verejného sektora¹⁷ a ochrany pred uchovávaním osobných údajov verejnými orgánmi¹⁸. Rešpektovanie súkromného života nie je absolútnym právom, keďže výkon práva na súkromie by mohol ohroziť iné práva, ako je sloboda prejavu a právo na prístup k informáciám, a naopak. ESĽP sa preto snaží nájsť rovnováhu medzi týmito rôznymi právami. Vysvetlil, že z článku 8 ECHR nielenže pre štáty vyplýva záväzok, aby sa zdržali akýchkoľvek krokov, ktorými by mohli porušiť toto právo zakotvené v Dohovore, ale za určitých okolností sa im ním ukladá pozitívna povinnosť aktívne zaistiť účinné rešpektovanie súkromného a rodinného života¹⁹. Viaceré z týchto prípadov sa podrobnejšie opisujú v príslušných kapitolách.

1.1.4. Dohovor Rady Európy č. 108

Vznik informačných technológií v 60. rokoch minulého storočia priniesol čoraz naliehavejšiu potrebu prijať podrobné pravidlá ochrany jednotlivcov formou ochrany ich osobných údajov. V polovici 70. rokov prijal Výbor ministrov Rady Európy viacero

15 Rada Európy, *Európsky dohovor o ľudských právach*, CETS č. 005, 1950.

16 Pozri napríklad: ESĽP, *Malone/Spojené kráľovstvo*, č. 8691/79, 2. augusta 1984; ESĽP, *Copland/Spojené kráľovstvo*, č. 62617/00, 3. apríla 2007, alebo ESĽP, *Mustafa Sezgin Tanrikulu/Turecko*, č. 27473/06, 18. júla 2017.

17 Pozri napríklad: ESĽP, *Klass a i./Nemecko*, č. 5029/71, 6. septembra 1978; ESĽP, *Uzun/Nemecko*, č. 35623/05, 2. septembra 2010.

18 Pozri napríklad: ESĽP, *Roman Zakharov/Rusko*, č. 47143/06, 4. decembra 2015; ESĽP, *Szabó a Vissy/Maďarsko*, č. 37138/14, 12. januára 2016.

19 Pozri napríklad: ESĽP, *I./Fínsko*, č. 20511/03, 17. júla 2008; ESĽP, *K.U./Fínsko*, č. 2872/02, 2. decembra 2008.

uznesení o ochrane osobných údajov, v ktorých sa odkazovalo na článok 8 ECHR²⁰. V roku 1981 bol *Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor č. 108)*²¹ pripravený na podpísanie. Dohovor č. 108 bol, a naďalej zostáva, jediným právne záväzným medzinárodným dokumentom v oblasti ochrany údajov.

Dohovor č. 108 sa vzťahuje na spracúvanie osobných údajov v súkromnom, ako aj vo verejnom sektore, napríklad spracúvanie osobných údajov v súdnictve či orgánmi presadzovania práva. Chráni jednotlivca pred zneužitím, ktoré by mohlo sprevádzať spracúvanie osobných údajov, a zároveň sa ním má regulovať cezhraničný tok osobných údajov. Pokiaľ ide o spracúvanie osobných údajov, zásady stanovené v Dohovore sa týkajú predovšetkým spravodlivého a zákonného získavania a automatizovaného spracúvania údajov, ktoré sa uchovávali na špecifikované legitímne účely. Znamená to, že tieto údaje sa nepoužívajú na ciele nezlučiteľné s týmito účelmi ani sa neuchovávajú dlhšie, než je to nevyhnutne potrebné. Uvedenými zásadami sa upravuje aj kvalita údajov, predovšetkým to, že musia byť primerané, relevantné a nie neúmerne (primeranosť) a musia byť presné.

Okrem poskytnutia záruk týkajúcich sa spracúvania osobných údajov a povinností v oblasti bezpečnosti údajov sa v Dohovore zakazuje, ak neexistujú primerané právne záruky, spracúvanie tzv. citlivých údajov, napríklad o rase, politických postojoch, zdravotnom stave, náboženskom presvedčení, sexuálnom živote či záznamoch vedených v registri trestov určitej osoby.

V Dohovore je takisto zakotvené právo jednotlivca vedieť o uchovávaní údajov, ktoré sa ho týkajú, a podľa potreby môcť tieto údaje opraviť. Obmedzenie práv stanovených v Dohovore je možné len v prípadoch nadradených záujmov, napríklad štátnej bezpečnosti alebo obrany. Dohovor síce umožňuje voľný tok osobných údajov medzi jeho zmluvnými stranami, zároveň sa v ňom však ukládajú určité obmedzenia tohto toku pre štáty, v ktorých právna úprava nezabezpečuje primeranú ochranu.

Je potrebné uviesť, že Dohovor č. 108 je záväzný pre štáty, ktoré ho ratifikovali. Nepodlieha súdnemu dohľadu ESLP, ale bol zohľadnený v jeho judikatúre v kontexte

20 Rada Európy, Výbor ministrov (1973), *Uznesenie (73) 22* o ochrane súkromia jednotlivcov vo vzťahu k elektronickým databankám v súkromnom sektore, 26. septembra 1973; Rada Európy, Výbor ministrov (1974), *Uznesenie (74) 29* o ochrane súkromia jednotlivcov vo vzťahu k elektronickým databankám vo verejnom sektore, 20. septembra 1974.

21 Rada Európy, Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, ETS č. 108, 1981.

článku 8 ECHR. V priebehu rokov tento súd rozhodol, že ochrana osobných údajov je dôležitou súčasťou práva na rešpektovanie súkromného života (článok 8) a pri určovaní, či došlo k zásahu do tohto základného práva, sa riadi zásadami Dohovoru č. 108²².

Výbor ministrov RE prijal v záujme prehĺbenia všeobecných zásad a pravidiel stanovených v Dohovore č. 108 niekoľko odporúčaní, ktoré nie sú právne záväzné. Tieto odporúčania ovplyvnili vývoj právnych predpisov o ochrane údajov v Európe. Po dlhé roky bolo napríklad jediným nástrojom v Európe, ktorý poskytoval usmernenia týkajúce sa využívania osobných údajov v policajnom sektore, odporúčanie v oblasti polície²³. Zásady uvedené v tomto odporúčaní, ako sú prostriedky uchovávaní súborov s údajmi a potreba zaviesť jasné pravidlá týkajúce sa prístupu osôb k týmto súborom, sa ďalej rozvíjali a odrážajú sa v právnych predpisoch EÚ, ktoré po ňom nasledovali²⁴. Novšie odporúčania sa zameriavajú na riešenie výziev digitálneho veku – napríklad v súvislosti so spracúvaním údajov v kontexte zamestnanosti (pozri [kapitolu 9](#)).

Dohovor č. 108 ratifikovali všetky členské štáty EÚ. V roku 1999 boli navrhnuté zmeny Dohovoru umožňujúce EÚ stať sa zmluvnou stranou, ktoré však nikdy nenaobudli platnosť²⁵. V roku 2001 bol prijatý Dodatokový protokol k Dohovoru č. 108. Zavádzajú sa ním ustanovenia o cezhraničnom toku údajov pre strany, ktoré nie sú zmluvnými stranami Dohovoru (tzv. tretie krajiny), ako aj ustanovenia o povinnom zriadení národných dozorných orgánov pre ochranu údajov²⁶.

K Dohovoru č. 108 môžu pristúpiť aj strany, ktoré nie sú zmluvnými stranami RE. Potenciál Dohovoru ako všeobecnej normy a jeho otvorenosť by mohli slúžiť ako základ pri podporovaní ochrany údajov na celosvetovej úrovni. V súčasnosti je 51 štátov zmluvnými stranami Dohovoru č. 108. Patria k nim všetky členské štáty Rady

22 Pozri napríklad: ESLP, *Z./Finsko*, č. 22009/93, 25. februára 1997.

23 Rada Európy, Výbor ministrov (1987), Odporúčanie členským štátom Rec (87)15, ktorým sa upravuje používanie osobných údajov v policajnom sektore, Štrasburg, 17. septembra 1987.

24 Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Ú. v. ES L 281, 23.11.1995.

25 Rada Európy, dodatky k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (ETS č. 108) prijaté Výborom ministrov v Štrasburgu 15. júna 1999.

26 Rada Európy, Dodatokový protokol k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov týkajúci sa orgánov dozoru a cezhraničných tokov údajov, ETS č. 181, 2001. Po modernizácii Dohovoru č. 108 sa tento Protokol už neuplatňuje, keďže jeho ustanovenia sa aktualizovali a začlenili do modernizovaného Dohovoru č. 108.

Európy (47 krajín); Uruguaj, prvá mimoeurópska krajina, ktorá pristúpila k Dohovoru v auguste 2013, a Maurícius, Senegal a Tunisko, ktoré pristúpili v roku 2016 a 2017.

Dohovor nedávno prešiel procesom **modernizácie**. V roku 2011 sa uskutočnili verejné konzultácie, ktoré umožnili potvrdiť dva hlavné ciele tejto činnosti: posilnenie ochrany súkromia v digitálnej oblasti a upevnenie kontrolných mechanizmov Dohovoru. Proces modernizácie bol zameraný na tieto ciele a bol dokončený prijatím protokolu, ktorým sa mení Dohovor č. 108 (Protokol CETS č. 223). Tieto práce prebiehali súbežne s inými reformami medzinárodných nástrojov na ochranu údajov a súbežne s reformou pravidiel EÚ na ochranu údajov, ktorá sa začala v roku 2012. Normotvorcovia na úrovni Rady Európy a EÚ vynaložili maximálne úsilie na zabezpečenie súladu medzi týmito dvoma právnymi rámcami a ich zlučiteľnosti. Modernizáciou sa zachoval všeobecný a flexibilný charakter Dohovoru a posilnil sa jeho potenciál ako univerzálneho nástroja v oblasti právnych predpisov o ochrane údajov. Potvrdzujú a stabilizujú sa dôležité zásady a jednotlivcom sa poskytujú nové práva, pričom sa zároveň zvyšuje zodpovednosť subjektov, ktoré spracúvajú osobné údaje, a zabezpečuje sa ich väčšia zodpovednosť. Napríklad fyzické osoby, ktorých osobné údaje sa spracúvajú, majú právo byť informované o dôvodoch takehoto spracúvania údajov a právo namietat proti tomuto spracúvaniu. V záujme boja proti zvýšenému využívaniu profilovania v online prostredí sa v Dohovore stanovuje aj právo jednotlivca, aby sa na neho nevzťahovali rozhodnutia založené výlučne na automatizovanom spracúvaní bez toho, aby sa zohľadnil jeho názor. Pri uplatňovaní Dohovoru v praxi sa za kľúčové považuje účinné presadzovanie pravidiel ochrany údajov nezávislými dozornými orgánmi zmluvných strán. Na tento účel sa v modernizovanom Dohovore zdôrazňuje, že je potrebné, aby dozorné orgány mali účinné právomoci a funkcie a aby pri plnení svojej úlohy boli skutočne nezávislé.

1.1.5. Právne predpisy Európskej únie o ochrane údajov

Právne predpisy EÚ tvorí primárne a sekundárne právo EÚ. Zmluvy, predovšetkým Zmluva o Európskej únii (ZEU) a Zmluva o fungovaní Európskej únie (ZFEÚ), boli ratifikované všetkými členskými štátmi EÚ a tvoria „primárne právo EÚ“. Nariadenia, smernice a rozhodnutia EÚ prijímajú európske inštitúcie, ktorým bola na základe zmlúv udelená táto právomoc, a často sa nazývajú „sekundárnym právom EÚ“.

Ochrana údajov v primárnom práve EÚ

Pôvodné zmluvy o založení Európskych spoločenstiev neobsahujú žiadne odkazy na ľudské práva alebo ich ochranu, keďže Európske hospodárske spoločenstvo bolo pôvodne plánované ako regionálna organizácia zameraná na hospodársku integráciu a vytvorenie spoločného trhu. Základnou zásadou, o ktorú sa opiera vytvorenie a rozvoj Európskych spoločenstiev – a ktorá stále platí aj v súčasnosti –, je zásada prenesenia právomocí. Podľa tejto zásady EÚ koná len v medziach právomocí, ktoré na ňu preniesli členské štáty, ako sa uvádza v zmluvách EÚ. Na rozdiel od Rady Európy zmluvy EÚ neobsahujú žiadnu výslovnú právomoc v otázkach základných práv.

Keďže však SDEÚ boli predkladané veci v súvislosti s porušovaním ľudských práv v oblastiach v rámci pôsobnosti práva Únie, SDEÚ poskytoval dôležitý výklad týchto zmlúv. V záujme poskytnutia ochrany jednotlivcom boli základné práva zahrnuté do tzv. všeobecných zásad európskeho práva. Podľa SDEÚ tieto všeobecné zásady odrážajú podstatu ochrany ľudských práv zakotvenej v ústavách jednotlivých členských štátov a zmluvách o ochrane ľudských práv, najmä v ECHR. SDEÚ konštatoval, že sa tak zaistiť súlad právnych predpisov EÚ s uvedenými zásadami.

Európska únia si uvedomila, že jej politiky by mohli mať vplyv na ľudské práva a v rámci snahy o to, aby sa občania cítili k EÚ „bližšie“, v roku 2000 vyhlásila Chartu základných práv Európskej únie (Charta). Charta zahŕňa celý rad občianskych, politických, hospodárskych a sociálnych práv európskych občanov, pričom sa v nej spájajú ústavné tradície a medzinárodné záväzky spoločné pre členské štáty. Práva opísané v Charte sú rozdelené do šiestich oddielov: dôstojnosť, slobody, rovnosť, solidarita, občianstvo a spravodlivosť.

Charta bola pôvodne len politickým dokumentom, ale po nadobudnutí účinnosti Lisabonskej zmluvy 1. decembra 2009²⁷ sa stala právne záväznou²⁸ ako súčasť primárneho práva EÚ (pozri článok 6 ods. 1 ZEÚ). Ustanovenia Charty sú určené inštitúciám a orgánom EÚ a zaväzujú ich k tomu, aby pri plnení svojich povinností rešpektovali práva uvedené v Charte. Ustanovenia Charty zaväzujú aj členské štáty pri vykonávaní práva Únie.

27 Pozri konsolidovanú verziu, Európske spoločenstvá (2012), Zmluva o Európskej únii, Ú. v. EÚ C 326, 2012, ako aj Európske spoločenstvá (2012), ZFEÚ, Ú. v. EÚ C 326, 2012.

28 EÚ (2012), Charta základných práv Európskej únie, Ú. v. EÚ C 326, 2012.

V Charte sa nielen zaručuje rešpektovanie súkromného a rodinného života (článok 7), ale stanovuje aj právo na ochranu osobných údajov (článok 8). V Charte sa výslovne zvyšuje úroveň tejto ochrany na úroveň ochrany základného práva v rámci právnych predpisov EÚ. Inštitúcie a orgány EÚ musia toto právo dodržiavať a zaručovať, a týka sa to aj členských štátov pri vykonávaní práva Únie (článok 51 Charty). Článok 8 Charty, ktorý bol sformulovaný niekoľko rokov po prijatí smernice o ochrane údajov, treba chápať ako ustanovenie vyjadrujúce už existujúce právne predpisy EÚ o ochrane údajov. Preto sa v Charte nielen výslovne uvádza právo na ochranu údajov v článku 8 ods. 1, ale odkazuje sa v nej aj na hlavné zásady ochrany údajov (v článku 8 ods. 2). A napokon, v článku 8 ods. 3 Charty sa zaručuje kontrola vykonávania uvedených zásad nezávislým orgánom.

Prijatie Lisabonskej zmluvy je medzníkom vo vývoji právnych predpisov v oblasti ochrany údajov, a to nielen vďaka povýšeniu Charty na záväzný právny dokument na úrovni primárneho práva, ale aj vďaka stanoveniu práva na ochranu osobných údajov. Toto právo sa osobitne stanovuje v článku 16 ZFEÚ, v časti zmluvy venovanej všeobecným zásadám EÚ. V článku 16 sa vytvára aj nový právny základ, ktorým sa EÚ udeľuje právomoc prijímať právne predpisy v oblasti ochrany údajov. Ide o dôležitý vývoj, pretože pravidlá EÚ na ochranu údajov, najmä smernica o ochrane údajov, boli pôvodne založené na právnom základe pre vnútorný trh a na potrebe aproximovať vnútroštátne právne predpisy, aby nedošlo k obmedzeniu voľného pohybu údajov v rámci EÚ. V článku 16 ZFEÚ sa stanovuje nezávislý právny základ pre moderný, komplexný prístup k ochrane údajov, ktorý zahŕňa všetky oblasti právomoci EÚ vrátane policajnej a justičnej spolupráce v trestných veciach. V článku 16 ZFEÚ sa tiež potvrdzuje, že dodržiavanie pravidiel ochrany údajov prijatých na jeho základe musí podliehať kontrole nezávislých dozorných orgánov. Článok 16 slúžil ako právny základ pre prijatie komplexnej reformy pravidiel ochrany údajov v roku 2016, t. j. všeobecného nariadenia o ochrane údajov a smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní (pozri ďalej).

Všeobecné nariadenie o ochrane údajov

Od roku 1995 do mája 2018 bola hlavným právnym nástrojom EÚ v oblasti ochrany údajov smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (smernica o ochrane údajov)²⁹. Bola prijatá v roku 1995, v čase, keď

²⁹ Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Ú. v. E S L 281, 1995.

už niektoré členské štáty mali vnútroštátne právne predpisy o ochrane údajov³⁰, a vyplynula z potreby harmonizovať tieto právne predpisy s cieľom zabezpečiť vysokú úroveň ochrany a voľný tok osobných údajov medzi jednotlivými členskými štátmi. Voľný pohyb tovaru, kapitálu, služieb a osôb v rámci vnútorného trhu si vyžadoval voľný tok údajov, ktorý by sa nemohol uskutočniť, keby sa členské štáty nemohli spolať na jednotnú vysokú úroveň ochrany údajov.

V smernici o ochrane údajov sa zohľadňovali zásady ochrany údajov, ktoré už sú obsiahnuté vo vnútroštátnych právnych predpisoch a v Dohovore č. 108, pričom sa tieto zásady často rozširovali. Využila sa tu možnosť rozšíriť nástroje ochrany podľa článku 11 Dohovoru č. 108. Ukázalo sa, že dôležitým prínosom k efektívnemu fungovaniu európskych právnych predpisov o ochrane údajov bolo najmä to, že v smernici sa zaviedol nezávislý dohľad ako nástroj na zlepšenie dodržiavania súladu s týmito predpismi. Tento prvok bol v roku 2001 následne prevzatý do právnych predpisov RE, a to prijatím Dodatočného protokolu k Dohovoru č. 108. To poukazuje na úzke prepojenie a vzájomný pozitívny vplyv týchto dvoch nástrojov v priebehu rokov.

V smernici o ochrane údajov sa stanovil podrobný a komplexný systém ochrany údajov v rámci EÚ. V súlade s právnym systémom EÚ sa však smernice neuplatňujú priamo a musia sa transponovať do vnútroštátnych právnych predpisov členských štátov. Členské štáty majú pri transpozícii ustanovení smernice nevyhnutne priestor na voľné uváženie. Napriek tomu, že smernica mala zabezpečiť úplnú harmonizáciu³¹ (a úplnú úroveň ochrany), v praxi bola v jednotlivých členských štátoch transponovaná rozdielne. Viedlo to k vytvoreniu rozdielnych pravidiel ochrany údajov v rámci EÚ, s odlišnými vymedzeniami pojmov a výkladom pravidiel v jednotlivých vnútroštátnych právnych predpisoch. Okrem toho sa líšili aj úrovne presadzovania a prísnosť sankcií v jednotlivých členských štátoch. Od vypracovania tejto smernice v polovici 90. rokov minulého storočia navyše došlo k významným zmenám informačných technológií. Všetky tieto dôvody spolu viedli k reforme právnych predpisov EÚ v oblasti ochrany údajov.

30 Nemecká spolková krajina Hesensko prijala v roku 1970 prvý zákon o ochrane údajov na svete, ktorý sa uplatňoval len v tejto spolkovej krajine. Švédsko prijalo zákon *Datalagen* v roku 1973; Nemecko prijalo spolkový zákon *Bundesdatenschutzgesetz* v roku 1976; a Francúzsko prijalo zákon *Loi relatif à l'informatique, aux fichiers et aux libertés* v roku 1977. V Spojenom kráľovstve bol zákon o ochrane údajov prijatý v roku 1984. A napokon, Holandsko prijalo zákon *Wet Persoonregistraties* v roku 1989.

31 SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECMD)/Administración del Estado*, 24. novembra 2011, bod 29.

Reforma viedla po rokoch intenzívnych diskusií k tomu, že v apríli 2016 bolo prijaté všeobecné nariadenie o ochrane údajov. Diskusie o potrebe modernizácie pravidiel EÚ na ochranu údajov sa začali v roku 2009, keď Komisia začala verejné konzultácie o budúcom právnom rámci pre základné právo na ochranu osobných údajov. Návrh nariadenia Komisia uverejnila v januári 2012, pričom sa začal dlhý legislatívny postup rokovaní medzi Európskym parlamentom a Radou EÚ. Vo všeobecnom nariadení o ochrane údajov sa po jeho prijatí stanovovalo dvojročné prechodné obdobie. V plnom rozsahu sa začalo uplatňovať od 25. mája 2018, čím sa zrušila smernica o ochrane údajov.

Prijatím všeobecného nariadenia o ochrane údajov v roku 2016 sa zmodernizovali právne predpisy EÚ v oblasti ochrany údajov, aby umožňovali ochranu základných práv na pozadí hospodárskych a sociálnych výziev digitálneho veku. GDPR zachováva a rozvíja základné zásady a práva dotknutej osoby stanovené v smernici o ochrane údajov. Okrem toho sa v ňom zavádzajú nové povinnosti týkajúce sa zavedenia špecificky navrhutej a štandardnej ochrany údajov, určenia zodpovednej osoby za určitých okolností, dodržiavania nového práva na prenosnosť údajov a dodržiavania zásady zodpovednosti. Podľa práva Únie sú nariadenia priamo uplatniteľné bez potreby ich vykonávania formou vnútroštátnej právnej úpravy. Vo všeobecnom nariadení o ochrane údajov sa tak stanovuje jednotný súbor pravidiel ochrany údajov pre celú EÚ. Vytvárajú sa tak jednotné pravidlá ochrany údajov v celej EÚ a prostredie právnej istoty, ktoré môže byť prospešné pre hospodárske subjekty a jednotlivcov ako „dotknuté osoby“.

Hoci je však všeobecné nariadenie o ochrane údajov priamo uplatniteľné, od členských štátov sa očakáva, že aktualizujú svoje existujúce vnútroštátne právne predpisy o ochrane údajov, aby dosiahli úplný súlad s týmto nariadením, zároveň sa však v jeho odôvodnení 10 zohľadňuje priestor na voľné uváženie v prípade osobitných ustanovení. Hlavné pravidlá a zásady stanovené v tomto nariadení, ako aj účinné práva, ktoré poskytuje jednotlivcom, predstavujú veľkú časť tejto príručky a sú opísané v nasledujúcich kapitolách. Nariadenie obsahuje komplexné pravidlá týkajúce sa územnej pôsobnosti. Vztahuje sa na podniky usadené v EÚ a vztahuje sa aj na prevádzkovateľov a sprostredkovateľov, ktorí nie sú usadení v EÚ, ale ktorí ponúkajú tovary alebo služby dotknutým osobám v EÚ alebo sledujú ich správanie. Keďže viaceré zámorské technologické spoločnosti majú na európskom trhu významný podiel a milióny zákazníkov v EÚ, podrobenie týchto organizácií pravidlám EÚ na ochranu údajov je dôležité na zabezpečenie ochrany jednotlivcov, ako aj zabezpečenie rovnakých podmienok.

Ochrana údajov v oblasti presadzovania práva – smernica 2016/680

Zrušená smernica o ochrane údajov zabezpečovala komplexný režim ochrany údajov. Tento režim bol teraz posilnený prijatím všeobecného nariadenia o ochrane údajov. Zrušená smernica o ochrane údajov bola síce komplexná, jej rozsah pôsobnosti však bol obmedzený na činnosti v rámci vnútorného trhu a na činnosti orgánov verejnej moci, ktoré nie sú orgánmi presadzovania práva. Na dosiahnutie potrebnej jednoznačnosti a rovnováhy medzi ochranou údajov a inými legitímnymi záujmami a na riešenie problémov, ktoré sú obzvlášť relevantné v konkrétnych sektoroch, preto bolo potrebné prijatie osobitných nástrojov. Patria k nim aj pravidlá, ktorými sa riadi spracúvanie osobných údajov orgánmi presadzovania práva.

Prvým právnym nástrojom EÚ, ktorým sa táto záležitosť upravovala, bolo rámcové rozhodnutie Rady 2008/977/SVV o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach. Jeho pravidlá sa uplatňovali len na výmenu údajov policajných a justičných orgánov medzi členskými štátmi. Vnútroštátne spracúvanie osobných údajov v rámci presadzovania práva bolo z rozsahu jeho pôsobnosti vylúčené.

Smernicou 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov³², nazývaná aj smernica o ochrane údajov pre orgány polície a trestného súdnictva, sa táto situácia napravila. Bola prijatá súčasne so všeobecným nariadením o ochrane údajov a zrušilo sa ňou rámcové rozhodnutie 2008/977/SVV, zaviedol sa komplexný systém ochrany osobných údajov v kontexte presadzovania práva a zároveň sa uznali osobitosti spracúvania údajov súvisiacich s verejnou bezpečnosťou. Hoci sa vo všeobecnom nariadení o ochrane údajov stanovujú všeobecné pravidlá na ochranu jednotlivcov pri spracúvaní ich osobných údajov a na zabezpečenie voľného pohybu takýchto údajov v rámci EÚ, v smernici sa stanovujú osobitné pravidlá ochrany údajov v oblasti justičnej spolupráce v trestných veciach a policajnej spolupráce. Ak príslušný orgán spracúva osobné údaje na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, uplatňuje sa smernica 2016/680. Ak príslušné orgány spracúvajú osobné údaje na iné ako uvedené účely, uplatňuje sa všeobecný režim podľa všeobecného nariadenia o ochrane

32 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov, Ú. v. EÚ L 119, 4.5.2016.

údajov. Na rozdiel od predchádzajúcej právnej úpravy (rámcové rozhodnutie Rady 2008/977/SVV) sa pôsobnosť smernice 2016/680 rozširuje na vnútroštátne spracúvanie osobných údajov orgánmi presadzovania práva a neobmedzuje sa na výmenu takýchto údajov medzi členskými štátmi. Okrem toho je cieľom smernice dosiahnuť rovnováhu medzi právami jednotlivcov a legitímnymi cieľmi spracúvania súvisiacimi s bezpečnosťou.

Na tento účel sa v smernici potvrdzuje právo na ochranu osobných údajov a základné zásady, ktoré by sa mali vzťahovať na spracúvanie údajov, a to v súlade s pravidlami a zásadami zakotvenými vo všeobecnom nariadení o ochrane údajov. Práva jednotlivcov a povinnosti uložené prevádzkovateľom – napríklad v súvislosti s bezpečnosťou údajov, špecificky navrhnutou a štandardnou ochranou údajov a oznamovaním porušení ochrany údajov –, sú podobné právam a povinnostiam stanoveným vo všeobecnom nariadení o ochrane údajov. V smernici sa takisto zohľadňujú novovznikajúce technologické výzvy, ktoré môžu mať mimoriadne závažný vplyv na jednotlivcov, ako je používanie metód profilovania orgánmi presadzovania práva. Rozhodnutia založené výlučne na automatizovanom spracúvaní vrátane profilovania sa v zásade zakazujú³³. Okrem toho nesmú byť založené na citlivých údajoch. V smernici sa k týmto zásadám stanovujú určité výnimky. Okrem toho takéto spracúvanie nesmie viesť k diskriminácii žiadnej osoby³⁴.

Smernica ďalej obsahuje pravidlá na zabezpečenie zodpovednosti prevádzkovateľov. Musia určiť zodpovednú osobu na monitorovanie dodržiavania pravidiel ochrany údajov, poskytovanie informácií a poradenstva prevádzkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie, o ich povinnostiach a na spoluprácu s dozorným orgánom. Spracúvanie osobných údajov v oblasti polície a trestného súdnictva v súčasnosti podlieha dohľadu nezávislých dozorných orgánov. Všeobecný právny režim ochrany údajov a osobitný režim ochrany údajov pre oblasť presadzovania práva a trestných vecí musia rovnako spĺňať požiadavky Charty základných práv EÚ.

Osobitný režim pre spracúvanie údajov v kontexte policajnej a justičnej spolupráce stanovený v smernici o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sa podrobne opisuje v kapitole 8.

33 Smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, článok 11 ods. 1.

34 Tamže, článok 11 ods. 2 a 3.

Smernica o súkromí a elektronických komunikáciách

Aj v sektore elektronických komunikácií bolo potrebné stanoviť osobitné pravidlá ochrany údajov. V súvislosti s rozmachom internetu, pevných liniek a mobilných telefónov je dôležité zabezpečiť, aby sa rešpektovali práva používateľov na súkromie a dôvernosť. V smernici 2002/58/ES³⁵ týkajúcej sa spracúvania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách alebo smernica o ePrivacy) sa stanovujú pravidlá bezpečnosti osobných údajov v týchto sieťach, oznamovanie porušení ochrany osobných údajov a dôvernosti komunikácií.

Pokiaľ ide o bezpečnosť, prevádzkovatelia elektronických komunikačných služieb musia okrem iného zabezpečiť, aby bol prístup k osobným údajom obmedzený len na oprávnené osoby, a prijať opatrenia na zabránenie zničeniu, strate alebo náhodnému poškodeniu osobných údajov³⁶. V prípade osobitného rizika narušenia bezpečnosti verejnej komunikačnej siete musia prevádzkovatelia informovať účastníkov o takomto riziku³⁷. Ak napriek prijatým bezpečnostným opatreniam dôjde k narušeniu bezpečnosti, prevádzkovatelia musia o porušení ochrany osobných údajov informovať príslušný vnútroštátny orgán poverený vykonávaním a presadzovaním smernice. Prevádzkovatelia sú niekedy povinní oznamovať prípady porušenia ochrany osobných údajov aj jednotlivcom, konkrétne ak je pravdepodobné, že porušenie negatívne ovplyvní ich osobné údaje alebo súkromie³⁸. Dôvernosť komunikácií si vyžaduje, aby sa v zásade zakázalo počúvanie, odpočúvanie, uchovávanie alebo iný druh zachytávania alebo sledovania komunikácie a metaúdajov. V tejto smernici sa zakazujú aj nevyžiadané správy (často označované ako „spam“), s výnimkou prípadov so súhlasom používateľov, a uvádzajú sa aj pravidlá týkajúce sa uchovávania „súborov cookie“ v počítačoch a zariadeniach. Z týchto hlavných negatívnych povinností jasne vyplýva, že dôvernosť komunikácie je výrazne spojená s ochranou práva na rešpektovanie súkromného života zakotveným v článku 7 Charty a právom na ochranu osobných údajov zakotveným v článku 8 Charty.

V januári 2017 Komisia uverejnila návrh nariadenia o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách, ktorým by sa mala nahradiť smernica o súkromí a elektronických komunikáciách. Cieľom tejto

35 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracúvania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, Ú. v. ES L 201 (smernica o súkromí a elektronických komunikáciách alebo smernica o ePrivacy).

36 Smernica o súkromí a elektronických komunikáciách, článok 4 ods. 1.

37 Tamže, článok 4 ods. 2.

38 Tamže, článok 4 ods. 3.

reformy je zosúladiť pravidlá upravujúce elektronické komunikácie s novým režimom ochrany údajov stanoveným v rámci všeobecného nariadenia o ochrane údajov. Nové nariadenie bude priamo uplatniteľné v celej EÚ; na všetkých jednotlivcov sa bude vzťahovať rovnaká úroveň ochrany ich elektronických komunikácií, zatiaľ čo pre telekomunikačných operátorov a podniky bude prínosom jednoznačnosť, právna istota a existencia jednotného súboru pravidiel pre celú EÚ. Navrhované pravidlá dôverylosti elektronických komunikácií sa budú vzťahovať aj na nových aktérov poskytujúcich elektronické komunikačné služby, na ktorých sa nevzťahuje smernica o súde a elektronických komunikáciách. Táto smernica sa vzťahovala len na tradičných poskytovateľov telekomunikačných služieb. Vzhľadom na rozsiahle využívanie služieb, ako sú Skype, WhatsApp, Facebook Messenger a Viber na zasielanie správ alebo hovorov, budú tieto služby over-the-top (služby OTT) patriť do rozsahu pôsobnosti tohto nariadenia a budú musieť spĺňať jeho požiadavky na ochranu údajov, súkromie a bezpečnosť. V čase uverejnenia tejto príručky ešte stále prebiehal legislatívny proces týkajúci sa pravidiel ochrany súkromia a elektronických komunikácií.

Nariadenie (EÚ) č. 45/2001

Keďže smernica o ochrane údajov sa mohla vzťahovať len na členské štáty EÚ, bol potrebný ďalší právny nástroj na zakotvenie ochrany údajov pri spracúvaní osobných údajov inštitúciami a orgánmi EÚ. Túto úlohu plní nariadenie (ES) č. 45/2001 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (nariadenie o ochrane údajov inštitúciami EÚ)³⁹.

Nariadenie č. 45/2001 dôkladne sleduje zásady všeobecného režimu ochrany údajov v EÚ a tieto zásady sa uplatňujú na spracúvanie údajov vykonávané inštitúciami a orgánmi EÚ pri výkone ich funkcií. Okrem toho sa zriaďuje nezávislý dozorný orgán, Európsky dozorný úradník pre ochranu údajov (EDPS), ktorý monitoruje uplatňovanie ustanovení tohto nariadenia. EDPS má právomoci v oblasti dohľadu a má povinnosť monitorovať spracúvanie osobných údajov v inštitúciách a orgánoch EÚ a predjednávať a vyšetrovať sťažnosti týkajúce sa údajného porušovania pravidiel ochrany údajov. Poskytuje aj poradenstvo inštitúciám a orgánom EÚ vo všetkých otázkach týkajúcich sa ochrany osobných údajov, a to od návrhov nových právnych predpisov až po vypracovanie interných pravidiel týkajúcich sa spracúvania údajov.

³⁹ Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov, Ú. v. ES L 8, 2001.

V januári 2017 Európska komisia predložila návrh nového nariadenia o spracúvaní údajov inštitúciami EÚ, ktorým sa zruší súčasné nariadenie. Tak ako pri reforme smernice o súkromí a elektronických komunikáciách, reformou nariadenia č. 45/2001 sa zmodernizujú a zosúladiť jeho pravidlá s novým režimom ochrany údajov stanoveným vo všeobecnom nariadení o ochrane údajov.

Úloha Súdneho dvora Európskej únie (SDEÚ)

SDEÚ má právomoc rozhodovať o tom, či členský štát splnil alebo nesplnil svoje povinnosti vyplývajúce z právnych predpisov EÚ o ochrane údajov, a právomoc vykladať právne predpisy EÚ s cieľom zabezpečiť ich účinné a jednotné uplatňovanie vo všetkých členských štátoch. Od prijatia smernice o ochrane údajov v roku 1995 došlo k nahromadeniu rozsiahleho súboru judikatúry, v ktorom sa objasňuje rozsah a význam zásad ochrany údajov a základné právo na ochranu osobných údajov zakotvené v článku 8 Charty. Napriek tomu, že táto smernica bola zrušená a v súčasnosti sa uplatňuje nový právny nástroj, ktorým je všeobecné nariadenie o ochrane údajov, táto existujúca judikatúra je naďalej relevantná a platná, pokiaľ ide o výklad a uplatňovanie zásad EÚ v oblasti ochrany údajov v rozsahu, v akom boli základné zásady a koncepcie smernice o ochrane údajov zachované v GDPR.

1.2. Obmedzenia práva na ochranu osobných údajov

Hlavné body

- Právo na ochranu údajov nie je absolútne právo, môže byť obmedzené, ak je to nevyhnutné na dosiahnutie cieľa všeobecného záujmu alebo na ochranu práv a slobôd iných.
- Podmienky obmedzenia práva na rešpektovanie súkromného života a na ochranu osobných údajov sú uvedené v článku 8 ECHR a v článku 52 ods. 1 Charty. Sú vyvíjané na základe výkladu judikatúry ESLP a SDEÚ.
- Podľa právnych predpisov RE o ochrane údajov spracúvanie osobných údajov predstavuje zákonné zasahovanie do práva na rešpektovanie súkromného života a môže sa vykonať len vtedy, ak:
 - je v súlade s právnymi predpismi,
 - sleduje legitímny cieľ,

- rešpektuje podstatu základných práv a slobôd,
- je nevyhnutné a primerané v demokratickej spoločnosti na dosiahnutie legitímneho účelu.
- V právnom poriadku EÚ sa stanovujú podobné podmienky týkajúce sa obmedzení výkonu základných práv chránených Chartou. Akékoľvek obmedzenie základného práva vrátane práva na ochranu osobných údajov môže byť zákonné, len ak:
 - je v súlade s právnymi predpismi,
 - rešpektuje podstatu tohto práva,
 - je nevyhnutné v súlade so zásadou proporcionality a
 - sleduje cieľ všeobecného záujmu uznaný EÚ alebo potrebu chrániť práva iných.

Základné právo na ochranu osobných údajov podľa článku 8 Charty nie je absolútnym právom, „ale musí sa zohľadniť so zreteľom na jeho funkciu v spoločnosti“⁴⁰. Článok 52 ods. 1 Charty uznáva, že výkon práv a slobôd uznaných v článkoch 7 a 8 Charty môže byť obmedzený, ak je také obmedzenie stanovené zákonom, rešpektuje podstatu týchto práv a slobôd, je dodržaná zásada proporcionality, je nevyhnutné a skutočne zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných⁴¹. Podobne v systéme ECHR je ochrana údajov zarúčená v článku 8 a výkon tohto práva môže byť v prípade potreby obmedzený, ak je to nevyhnutné na sledovanie legitímneho účelu. V tomto oddiele sa uvádzajú podmienky zasahovania podľa ECHR, ako ich vykladá judikatúra ESĽP, ako aj podmienky zákonných obmedzení podľa článku 52 Charty.

1.2.1. Požiadavky na oprávnený zásah podľa ECHR

Spracúvanie osobných údajov môže predstavovať zásah do práva dotknutej osoby na rešpektovanie súkromného života, ktoré je chránené článkom 8 ECHR⁴². Ako už bolo vysvetlené (pozri [oddiel 1.1.1](#) a [oddiel 1.1.4](#)), na rozdiel od právneho poriadku EÚ sa v ECHR nezakotvuje ochrana osobných údajov ako samostatné základné právo. Ochrana osobných údajov je namiesto toho súčasťou práv chránených v rámci práva na rešpektovanie súkromného života. Preto do rozsahu pôsobnosti článku 8 ECHR

40 Pozri napríklad SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010, bod 48.

41 Tamže, bod 50.

42 ESĽP, *S. a Marper/Spojené kráľovstvo* [VK], č. 30562/04 a č. 30566/04, 8. decembra 2008, bod 67.

nepatrí nevyhnutne každá operácia zahŕňajúca spracúvanie osobných údajov. Pri uplatňovaní článku 8 je najprv potrebné určiť, či bol ohrozený súkromný záujem alebo súkromný život príslušnej osoby. ESĽP vo svojej judikatúre považuje pojem „súkromný život“ za široký pojem, ktorý zahŕňa aj aspekty profesionálneho života a správania na verejnosti. Tento súd takisto rozhodol, že ochrana osobných údajov je dôležitou súčasťou práva na rešpektovanie súkromného života. Napriek širokému výkladu pojmu súkromného života by však nie všetky druhy spracúvania samy osebe mohli ohroziť práva chránené podľa článku 8.

V prípade, že sa ESĽP domnieva, že daná spracovateľská operácia ovplyvňuje právo jednotlivca na rešpektovanie súkromného života, preskúma, či je zásah oprávnený. Právo na rešpektovanie súkromného života nie je absolútnym právom, ale musí byť vyvážené a zosúladené s ďalšími oprávnenými záujmami a právami, buď iných osôb (súkromné záujmy), alebo spoločnosti ako celok (verejné záujmy).

Zásah by mohol byť oprávnený, ak kumulatívne platia tieto podmienky:

Súlad s právnymi predpismi

Podľa judikatúry ESĽP je zásah v súlade s právnymi predpismi vtedy, keď je založený na ustanovení vnútroštátneho právneho predpisu, ktorý spĺňa určité vlastnosti. Príslušný právny predpis musí „byť prístupný dotknutým osobám a predvídateľný z hľadiska dôsledkov“⁴³. Právny predpis je predvídateľný, ak „je formulovaný dostatočne presne na to, aby umožnil jednotlivcovi (v prípade potreby za pomoci vhodných pokynov) prispôbiť jeho konanie“⁴⁴. Okrem toho, „stupeň presnosti, ktorý sa v tejto súvislosti od právneho predpisu požaduje, bude závisieť od konkrétneho predmetu“⁴⁵.

43 ESĽP, *Amann/Švajčiarsko* [VK], č. 27798/95, 16. februára 2000, bod 50; pozri tiež ESĽP, *Kopp/Švajčiarsko* č. 23224/94, 25. marca 1998, bod 55 a ESĽP, *Iordachi a i./Moldavsko*, č. 25198/02, 10. februára 2009, bod 50.

44 ESĽP, *Amann/Švajčiarsko* [VK], č. 27798/95, 16. februára 2000, bod 56; pozri tiež ESĽP, *Malone/Spojené kráľovstvo*, č. 8691/79, 2. augusta 1984, bod 66; ESĽP, *Silver a i./Spojené kráľovstvo*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marca 1983, bod 88.

45 ESĽP, *The Sunday Times/Spojené kráľovstvo*, č. 6538/74, 26. apríla 1979, bod 49; pozri tiež ESĽP, *Silver a i./Spojené kráľovstvo*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marca 1983, bod 88.

Príklady: Sťažovateľ vo veci *Rotaru/Rumunsko*⁴⁶ tvrdil, že došlo k porušeniu jeho práva na rešpektovanie súkromného života tým, že rumunská spravodajská služba mala k dispozícii a používala spis obsahujúci jeho osobné informácie. EŠLP dospel k záveru, že hoci vnútroštátne právne predpisy umožňovali zhromažďovanie, zaznamenávanie a archivovanie utajených súborov informácií týkajúcich sa národnej bezpečnosti, nestanovovali sa v nich žiadne obmedzenia výkonu týchto právomocí, ktoré záviseli od voľného uváženia týchto orgánov. Vo vnútroštátnych právnych predpisoch napríklad nebol vymedzený druh informácií, ktoré je možné spracúvať, kategórie osôb, proti ktorým je možné nariadiť sledovanie, okolnosti, za ktorých je možné takéto opatrenia prijať, či postup, ktorý treba dodržať. Súdny dvor preto dospel k záveru, že vnútroštátne právne predpisy nespĺňajú požiadavku predvídateľnosti podľa článku 8 ECHR a že došlo k porušeniu uvedeného článku.

Vo veci *Taylor-Sabori/Spojené kráľovstvo*⁴⁷ bol sťažovateľ sledovaný políciou. Pomocou „klonu“ jeho pagera polícia dokázala zachytávať správy, ktoré mu boli doručené. Sťažovateľ bol následne zatknutý a obvinený zo spolčenia s cieľom dodávať kontrolovanú drogu. Časť obžaloby vychádzala z paralelne písomne zaznamenávaných správ z pagera, ktoré polícia prepísala. V čase konania súdneho sporu sťažovateľa britské právne predpisy neobsahovali žiadne ustanovenie, ktorým by sa upravovalo zachytávanie komunikácie prenášanej prostredníctvom súkromného telekomunikačného systému. Zásah do práv sťažovateľa teda nebol „v súlade s právnymi predpismi“. EŠLP dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Vo veci *Vukota-Bojić/Švajčiarsko*⁴⁸ išlo o tajné sledovanie žiadateľa o sociálne poistenie zo strany súkromných detektívov, ktorých najala príslušná poisťovňa. EŠLP rozhodol, že hoci opatrenie týkajúce sa sledovania, o ktoré ide v sťažnosti, bolo nariadené súkromnou poisťovňou, táto spoločnosť bola oprávnená štátom na poskytovanie dávok vyplývajúcich z povinného zdravotného poistenia a na výber poistného. Štát sa nezbujaňuje zodpovednosti podľa Dohovoru tým, že svoje povinnosti prenesie na súkromné subjekty alebo jednotlivcov. Vo vnútroštátnom práve musia byť stanovené dostatočné

46 EŠLP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000, bod 57; pozri tiež EŠLP, *Association for European Integration and Human Rights a Ekimdziev/Bulharsko*, č. 62540/00, 28. júna 2007; EŠLP, *Shimovolos/Rusko*, č. 30194/09, 21. júna 2011; a EŠLP, *Vetter/Francúzsko*, č. 59842/00, 13. mája 2005.

47 EŠLP, *Taylor-Sabori/Spojené kráľovstvo*, č. 47114/99, 22. októbra 2002.

48 EŠLP, *Vukota-Bojić/Švajčiarsko*, č. 61838/10, 18. októbra 2016, bod 77.

záruky proti zneužitiu tak, aby zásah do práv podľa článku 8 ECHR bol „v súlade s právnymi predpismi“. V tomto prípade ESĽP dospel k záveru, že došlo k porušeniu článku 8 ECHR, pretože vo vnútroštátnych právnych predpisoch nebol dostatočne objasnený rozsah a spôsob uplatňovania voľnej úvahy priznanej poisťovníam, ktoré konajú ako orgány verejnej moci v sporoch týkajúcich sa poistného pri vykonávaní tajného sledovania poistenej osoby. Vnútroštátne právne predpisy najmä nezahŕňali dostatočné záruky proti zneužitiu.

Sledovanie legitímneho cieľa

Legitímnym cieľom môže byť niektorý z uvedených verejných záujmov alebo ochrana práv a slobôd iných. Legitímne ciele, ktoré by mohli odôvodniť zásah, sú podľa článku 8 ods. 2 ECHR v záujme národnej bezpečnosti, verejnej bezpečnosti alebo hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinosti, ochrany zdravia alebo morálky a ochrany práv a slobôd iných osôb.

Príklad: Sťažovateľ vo veci *Peck/Spojené kráľovstvo*⁴⁹ sa pokúsil spáchať samovraždu tak, že si na ulici podrezal zápästia, pričom nevedel o tom, že tento pokus zaznamenal kamerový systém. Príslušníci polície, ktorí záznamy kamerového systému sledovali, sťažovateľa zachránili a následne poskytli záznam kamerového systému médiám, ktoré ho zverejnili bez zahalenia tváre sťažovateľa. ESĽP dospel k záveru, že neexistovali žiadne relevantné ani dostatočné dôvody, ktoré by oprávňovali orgány priamo zverejniť záznam bez súhlasu sťažovateľa alebo utajenia jeho totožnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Nevyhnutosť v demokratickej spoločnosti

ESĽP konštatoval, že „z pojmu nevyhnutnosti vyplýva, že zásah zodpovedá naliehavej spoločenskej potrebe, a najmä to, že je primeraný stanovenému legitímnemu cieľu“⁵⁰. Pri posudzovaní toho, či je opatrenie potrebné na riešenie naliehavej spoločenskej potreby, skúma ESĽP jeho relevantnosť a vhodnosť vo vzťahu k sledovaniu cieľu. Môže pritom zohľadniť, či sa zásah pokúša riešiť otázku, ktorá, ak ostane nevyriešená, by mohla mať škodlivý vplyv na spoločnosť, či existuje nejaký dôkaz,

49 ESĽP, *Peck/Spojené kráľovstvo*, č. 44647/98, 28. januára 2003, bod 85.

50 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987, bod 58.

že zásah môže zmierniť takýto škodlivý vplyv, a aký je širší pohľad spoločnosti na danú problematiku⁵¹. Napríklad získavanie a ukladanie osobných údajov konkrétnych osôb, o ktorých sa zistilo, že sú napojené na teroristické hnutia, vykonávané bezpečnostnými službami, by bolo zásahom do práva jednotlivcov na rešpektovanie súkromného života, napriek tomu však tento zásah slúži vážnej, naliehavej sociálnej potrebe v oblasti národnej bezpečnosti a boja proti terorizmu. Splnenie kritéria nevyhnutnosti si vyžaduje, aby bol zásah aj primeraný. V judikatúre ESLP sa primeranosť rieši v rámci pojmu nevyhnutnosti. Primeranosť si vyžaduje, aby zásah do práv chránených podľa ECHR neprekročil rámec toho, čo je potrebné na dosiahnutie sledovaného legitímneho cieľa. Dôležitými faktormi, ktoré treba zohľadniť pri uplatňovaní kritéria primeranosti, je rozsah zásahu, najmä počet dotknutých osôb a záruky alebo výhrady zavedené s cieľom obmedziť jeho rozsah alebo škodlivé účinky na práva jednotlivcov⁵².

Príklad: Vo veci *Khelili/Švajčiarsko*⁵³ polícia počas policajnej kontroly zistila, že sťažovateľka má pri sebe vizitky, na ktorých bolo napísané: „Milá a pekná žena pred štyridsiatkou by sa rada zoznámila s mužom, ktorý by s ňou občas zašiel na pohárik alebo do spoločnosti. Tel. č. [...]“. Sťažovateľka tvrdila, že po nájdení vizitiek polícia zapísala jej meno do registra prostitútok, čo je zamestnanie, ktoré ona trvale popiera. Sťažovateľka požadovala odstránenie slova „prostitútka“ z policajných počítačových záznamov. ESLP v zásade uznal, že uchovávanie osobných údajov jednotlivca na základe skutočnosti, že táto osoba by mohla spáchať iný trestný čin, môže byť za určitých okolností primerané. V prípade sťažovateľky sa podozrenie z nezákonnej prostitúcie zdalo byť príliš neurčité a všeobecné, nebolo doložené konkrétnymi skutočnosťami, keďže sťažovateľka nikdy nebola odsúdená za nezákonnú prostitúciu, a teda nie je možné hovoriť o „naliehavej spoločenskej potrebe“ v zmysle článku 8 ECHR. Súd zohľadnil skutočnosť, že orgány mali overiť presnosť uchovávaných údajov o sťažovateľke, ako aj závažnosť zásahu do jej práv a skonštatoval, že dlhoročný zápis slova „prostitútka“ v policajných spisoch nebol nevyhnutný v demokratickej spoločnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

51 Pracovná skupina pre ochranu údajov zriadená podľa článku 29 (pracovná skupina zriadená podľa článku 29), *Stanovisko k uplatňovaniu zásad nevyhnutnosti a proporcionality a ochrany údajov v sektore presadzovania práva*, WP 211, Brusel, 27. februára 2014, s. 7 – 8.

52 Tamže, s. 9 – 11.

53 ESLP, *Khelili/Švajčiarsko*, č. 16188/07, 18. októbra 2011.

Príklad: Vo veci *S. a Marper/Spojené kráľovstvo*⁵⁴ boli obaja sťažovatelia zatknutí a obvinení zo spáchania trestných činov. Polícia im odobrala odtlačky prstov a vzorky DNA v súlade so zákonom o policajnej činnosti a dôkazoch o trestnej činnosti. Sťažovatelia neboli nikdy odsúdení: jeden bol zbavený obvinenia na súde a trestné konanie proti druhému sťažovateľovi bolo zastavené. Polícia im napriek tomu odobrala odtlačky prstov, profily DNA a bunkové vzorky a uchovávala ich v databáze, pričom na základe vnútroštátnych právnych predpisov bolo povolené ich uchovávanie bez časového obmedzenia. Hoci Spojené kráľovstvo tvrdilo, že uchovanie týchto informácií malo pomôcť pri identifikácii budúcich páchatelov, a teda sledovalo legitímny cieľ predchádzania trestnej činnosti a jej odhaľovania, ESĽP považoval zásah do práva sťažovateľov na rešpektovanie súkromného života za neoprávnený. Súd pripomenul, že základné zásady ochrany údajov si vyžadujú, aby uchovávanie osobných údajov bolo primerané vo vzťahu k účelu ich získania, a že doby uchovávania údajov musia byť obmedzené. Súd akceptoval tvrdenie, že rozšírenie databázy tak, aby zahŕňala profily DNA nielen odsúdených osôb, ale všetkých osôb, ktoré boli podozrivé, ale neboli odsúdené, by mohlo prispieť k odhaľovaniu a prevencii trestnej činnosti v Spojenom kráľovstve. Súd bol však prekvapený „všeobecným a nerozlišujúcim charakterom právomocí pri uchovávaní“⁵⁵.

Vzhľadom na množstvo genetických a zdravotných informácií obsiahnutých v bunkových vzorkách bol zásah do práva sťažovateľov na súkromný život obzvlášť rušivý. Zatknutým osobám bolo možné odoberať odtlačky prstov a vzorky a uchovávať ich na neobmedzené obdobie v policajnej databáze bez ohľadu na povahu a závažnosť trestného činu, a dokonca aj v prípade menej závažných trestných činov, za ktoré nemožno uložiť trest odňatia slobody. Okrem toho osoby, ktoré boli zbavené obvinenia, mali len obmedzené možnosti dosiahnuť odstránenie svojich údajov z databázy. ESĽP takisto osobitne zvážil skutočnosť, že jeden zo sťažovateľov bol pri zatknutí vo veku jedenásť rokov. Uchovávanie osobných údajov maloletej osoby, ktorá nebola odsúdená, môže byť obzvlášť škodlivé vzhľadom na jej zraniteľnosť a dôležitosť jej vývoja a začlenenia do spoločnosti⁵⁶. Súd jednomyselne rozhodol, že toto uchovávanie predstavuje neprimeraný zásah do práva na súkromný život, ktorý nemožno považovať za nevyhnutný v demokratickej spoločnosti.

54 ESĽP, *S. a Marper/Spojené kráľovstvo* [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008.

55 Tamže, bod 119.

56 Tamže, bod 124.

Príklad: ESLP vo veci *Leander/Švédsko*⁵⁷ rozhodol, že tajná previerka uchádzačov o pracovné miesta, ktoré sú dôležité z hľadiska národnej bezpečnosti, ako taká nie je v rozpore s požiadavkou nevyhnutnosti v demokratickej spoločnosti. Pokiaľ ide o osobitné záruky stanovené vo vnútroštátnych právnych predpisoch o ochrane záujmov dotknutých osôb, napríklad kontroly vykonávané parlamentom alebo ministrom spravodlivosti, ESLP dospel k záveru, že švédsky systém previerok zamestnancov spĺňa požiadavky článku 8 ods. 2 ECHR. Keďže žalovaný štát mal široký priestor na voľnú úvahu, bol oprávnený dospieť k záveru, že v prípade sťažovateľa záujmy národnej bezpečnosti prevažujú nad individuálnymi záujmami. Súd dospel k záveru, že nedošlo k porušeniu článku 8 ECHR.

1.2.2. Podmienky zákonných obmedzení podľa Charty základných práv EÚ

Štruktúra a znenie Charty sa líšia od ECHR. V Charte sa nepoužíva pojem zásahy do zaručených práv, ale obsahuje ustanovenie o obmedzení vykonávania práv a slobôd uznaných Chartou.

Podľa článku 52 ods. 1 sú obmedzenia výkonu práv a slobôd uznaných Chartou, a teda aj obmedzenia výkonu práva na ochranu osobných údajov, napríklad pri spracúvaní osobných údajov, prípustné len vtedy, keď:

- sú stanovené zákonom a
- rešpektujú podstatu práva na ochranu údajov, a
- sú nevyhnutné podľa zásady proporcionality⁵⁸, a
- zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou alebo sú potrebné na ochranu práv a slobôd iných.

Keďže ochrana osobných údajov predstavuje v právnom poriadku EÚ samostatné a nezávislé základné právo, chránené podľa článku 8 Charty, každé spracúvanie

⁵⁷ ESLP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987, body 59 a 67.

⁵⁸ K otázke posúdenia nevyhnutnosti opatrení obmedzujúcich základné právo na ochranu osobných údajov pozri: EDPS (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017.

osobných údajov samo osebe predstavuje zásah do tohto práva. Nezáleží na tom, či sa dotknuté osobné údaje týkajú súkromného života jednotlivca, či sú citlivé alebo či pre dotknutú osobu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky. Na to, aby bol zásah zákonný, musí byť v súlade so všetkými podmienkami uvedenými v článku 52 ods. 1 Charty.

Stanovené zákonom

Obmedzenia práva na ochranu osobných údajov musia byť stanovené zákonom. Z tejto požiadavky vyplýva, že obmedzenia musia byť založené na právnom základe, ktorý je primerane dostupný a predvídateľný a je dostatočne presný na to, aby jednotlivci dokázali pochopiť svoje povinnosti a prispôbiť svoje správanie. V právnom základe sa musí okrem toho jasne vymedzovať rozsah a spôsob výkonu právomoci príslušných orgánov, pokiaľ ide o ochranu jednotlivcov pred svojvoľným zásahom. Tento výklad sa podobá požiadavke „zákonného zásahu“ podľa judikatúry ESĽP⁵⁹ a existujú argumenty, že význam slovného spojenia „stanovené zákonom“, ktorý sa používa v Charte, by mal byť rovnaký ako význam, ktorý sa mu pripisuje v kontexte ECHR⁶⁰. Pri výklade rozsahu pôsobnosti článku 52 ods. 1 Charty je relevantné, aby SDEÚ zohľadnil judikatúru ESĽP a najmä pojem „kvalita právnych predpisov“, ktorý v nej bol v priebehu rokov vytvorený⁶¹.

Rešpektovanie podstaty práva

Podľa právneho poriadku Únie musí akékoľvek obmedzenie základných práv chránených Chartou rešpektovať podstatu týchto práv. Znamená to, že obmedzenia, ktoré sú také rozsiahle a rušivé, že by základné právo bolo zbavené jeho základného obsahu, nemôžu byť odôvodnené. Ak je podstata práva ohrozená, obmedzenie sa musí považovať za nezákonné, a to bez toho, aby bolo potrebné ďalej posudzovať, či slúži cieľu všeobecného záujmu a spĺňa kritériá nevyhnutnosti a proporcionality.

59 EDPS (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017, s. 4; pozri tiež SDEÚ, *Stanovisko 1/15 Súdneho dvora (veľká komora)*, 26. júla 2017.

60 SDEÚ, spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis, návrhy, ktoré predniesol generálny advokát Saugmandsgaard Øe*, 19. júla 2016, bod 140.

61 SDEÚ, C-70/10, *Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)*, návrhy, ktoré predniesol generálny advokát Cruz Villalón, 14. apríla 2011, bod 100.

Príklad: Vec *Schrems*⁶² sa týkala ochrany jednotlivcov pri prenose ich osobných údajov do tretích krajín – v tomto prípade do Spojených štátov amerických. Pán Schrems, rakúsky občan, ktorý je používateľom Facebooku už niekoľko rokov, podal sťažnosť na írsky dozorný orgán pre ochranu osobných údajov s cieľom odmietnuť prenos svojich osobných údajov z írskej dcérskej spoločnosti Facebook do spoločnosti Facebook Inc. a na servery nachádzajúce sa v USA, kde sa spracúvajú. Tvrdil, že vzhľadom na odhalenia pána Edwarda Snowdena, amerického oznamovateľa protispoločenskej činnosti, z roku 2013, ktoré sa týkali činností sledovania spravodajských služieb Spojených štátov, právo a prax v USA nezaistujú dostatočnú ochranu osobných údajov prenášaných na územie USA. Pán Snowden odhalil, že Národná bezpečnostná agentúra sa priamo napojila na servery spoločností, ako je Facebook, a mohla čítať obsah chatov a súkromných správ.

K prenosu údajov do USA dochádzalo na základe rozhodnutia Komisie o primeranosti, ktoré bolo prijaté v roku 2000 a ktoré umožňuje prenosy americkým spoločnostiam, ktoré osvedčia, že budú chrániť osobné údaje prenášané z EÚ a budú dodržiavať tzv. „zásady Safe Harbour“. Po predložení veci SDEÚ tento preskúmal platnosť rozhodnutia Komisie vzhľadom na Chartu. Pripomenul, že ochrana základných práv v EÚ si vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné. SDEÚ považoval právnu úpravu umožňujúcu orgánom verejnej moci všeobecný prístup k obsahu elektronických komunikácií za právnu úpravu, ktorá „zasahuje do podstaty obsahu základného práva na rešpektovanie súkromného života, ako je zaručené článkom 7 Charty“. Toto právo by bolo zásadne ohrozené, ak by americké orgány verejnej moci mohli náhodne získavať prístup k elektronickej komunikácii bez toho, aby museli uviesť objektívne odôvodnenie založené na dôvodoch z oblasti národnej bezpečnosti alebo predchádzania trestnej činnosti, ktoré by špecificky súviseli s dotknutými osobami, a to bez toho, aby sledovacie praktiky boli doplnené o akékoľvek primerané záruky proti zneužití právomoci.

Okrem toho „právna úprava, ktorá neupravuje nijakú možnosť osoby podliehajúcej súdnej právomoci uplatniť právne prostriedky nápravy, aby mala prístup k osobným údajom, ktoré sa jej týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov“, je nezlučiteľná so základným právom na účinnú súdnu ochranu (článok 47 Charty). Rozhodnutím o Safe Harbour sa teda zo

62 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

strany USA nezabezpečila úroveň ochrany základných práv, ktorá by bola v podstate rovnocenná úrovni zaručenej v rámci EÚ podľa smernice vykladanej v spojení s Chartou. SDEÚ následne zrušil platnosť tohto rozhodnutia⁶³.

Príklad: Vo veci *Digital Rights Ireland*⁶⁴ SDEÚ preskúmal zlučiteľnosť smernice 2006/24/ES (smernica o uchovávaní údajov) s článkami 7 a 8 Charty. V smernici sa ukladá poskytovateľom elektronických komunikačných služieb povinnosť uchovávať prevádzkové a lokalizačné údaje najmenej počas šiestich mesiacov a najviac 24 mesiacov a umožniť príslušným vnútroštátnym orgánom prístup k týmto údajom na účely prevencie, vyšetrovania, odhaľovania a stihania závažných trestných činov. Smernicou sa nepovoľovalo uchovávanie obsahu elektronických komunikácií. SDEÚ uviedol, že údaje, ktoré museli poskytovatelia uchovávať podľa tejto smernice, zahŕňali údaje potrebné na zistenie a identifikáciu zdroja komunikácie a adresáta komunikácie, na určenie dátumu, času a trvania komunikácie, telefónne číslo volajúceho a číslo volaného, ako aj IP adresu. Z týchto „všetkých údajov možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú“.

Uchovávanie údajov podľa tejto smernice preto predstavuje obzvlášť závažný zásah do práva na súkromie a na ochranu osobných údajov. SDEÚ však rozhodol, že tento zásah nemal nepriaznivý vplyv na podstatu týchto práv. Pokiaľ ide o právo na súkromie, jeho podstata nebola ohrozená, keďže smernica neumožňuje oboznámiť sa so samotným obsahom elektronickej komunikácie. Podobne nebola ohrozená ani podstata práva na ochranu osobných údajov, keďže v smernici sa vyžaduje od poskytovateľov elektronických komunikačných služieb, aby dodržiavali určité zásady ochrany údajov a bezpečnosti údajov a aby na tento účel prijali primerané technické a organizačné opatrenia.

63 Rozhodnutie SDEÚ o zrušení rozhodnutia Komisie 520/2000/ES bolo založené aj na iných dôvodoch, ktoré budú preskúmané v ďalších oddieloch tejto príručky. SDEÚ sa predovšetkým domnieval, že rozhodnutím sa protiprávne obmedzovali právomoci vnútroštátnych dozorných orgánov pre ochranu osobných údajov. Okrem toho v rámci režimu Safe Harbour jednotlivci nemali k dispozícii žiadne súdne prostriedky nápravy v prípade, že by chceli získať prístup k osobným údajom, ktoré sa ich týkajú, a/alebo dosiahnuť ich opravu alebo vymazanie. V dôsledku toho dochádzalo aj k zásahu do podstaty základného práva na účinnú súdnu ochranu, ako je upravené v článku 47 Charty.

64 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

Nevyhnutnosť a primeranosť

V článku 52 ods. 1 Charty sa stanovuje, že základné práva a slobody uznané v Charte možno obmedziť len vtedy, ak je to nevyhnutné a za predpokladu dodržiavania zásady proporcionality.

Obmedzenie môže byť **nevyhnutné**, ak je potrebné prijať opatrenia v záujme sledovaného cieľa verejného záujmu, ale nevyhnutnosť, ako ju vykladá SDEÚ, tiež znamená, že prijaté opatrenia musia byť menej rušivé v porovnaní s inými možnosťami na dosiahnutie tohto cieľa. Pokiaľ ide o obmedzenia práv na rešpektovanie súkromného života a ochranu osobných údajov, SDEÚ uplatňuje prísne kritérium nevyhnutnosti, pričom zastáva názor, že „odchýlky a obmedzenia sa musia uplatňovať len vtedy, ak je to prísne nevyhnutné“. Ak sa obmedzenie považuje za prísne nevyhnutné, takisto je potrebné posúdiť, či je toto obmedzenie primerané.

Primeranosť znamená, že výhody vyplývajúce z obmedzenia by mali prevážiť nad nevýhodami, ktoré obmedzenie spôsobuje pri výkone dotknutých základných práv⁶⁵. Je dôležité, aby obmedzenia obsahovali primerané záruky, aby sa znížili nevýhody a riziká pri uplatňovaní práv na súkromie a ochranu údajov.

Príklad: SDEÚ vo veci *Volker und Markus Schecke*⁶⁶ dospel k záveru, že uložením povinnosti zverejniť osobné údaje týkajúce sa všetkých fyzických osôb, ktoré boli príjemcami pomoci od určitých poľnohospodárskych fondov, bez rozlíšenia na základe relevantných kritérií, napríklad obdobia, v ktorom dané osoby poberali pomoc, frekvencie pomoci alebo jej povahy či výšky, Rada a Komisia nedodržali obmedzenia vyplývajúce zo zásady proporcionality.

Preto SDEÚ považoval za nutné vyhlásiť určité ustanovenia nariadenia Rady (ES) č. 1290/2005 za neplatné a vyhlásiť nariadenie č. 259/2008 za neplatné v celom jeho rozsahu⁶⁷.

⁶⁵ EDPS (2017), *Necessity Toolkit* s. 5.

⁶⁶ SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010, body 89 a 86.

⁶⁷ Nariadenie Rady (ES) č. 1290/2005 z 21. júna 2005 o financovaní Spoločnej poľnohospodárskej politiky, Ú. v. EÚ L 209, 2005; nariadenie Komisie (ES) č. 259/2008 z 18. marca 2008, ktorým sa stanovujú podrobné pravidlá uplatňovania nariadenia Rady (ES) č. 1290/2005 v súvislosti s uverejňovaním informácií o príjemateľoch pomoci zo zdrojov Európskeho poľnohospodárskeho záručného fondu (EPZF) a Európskeho poľnohospodárskeho fondu pre rozvoj vidieka (EPFRV), Ú. v. EÚ L 76, 2008.

Príklad: Vo veci *Digital Rights Ireland*⁶⁸ SDEÚ rozhodol, že zásah do práva na súkromie spôsobený smernicou o uchovávaní údajov neohrozuje podstatu tohto práva, keďže zakazuje uchovávanie obsahu elektronickej komunikácie. Dospel však aj k záveru, že táto smernica je nezlučiteľná s článkom 7 a 8 Charty, a vyhlásil ju za neplatnú. Vzhľadom na to, že agregované prevádzkové a lokalizačné údaje ako celok by sa mohli analyzovať a poskytnúť detailný obraz o súkromnom živote jednotlivcov, predstavovalo to závažný zásah do týchto práv. SDEÚ zohľadnil aj skutočnosť, že v smernici sa vyžaduje uchovávanie všetkých metaúdajov týkajúcich sa telefonického spojenia prostredníctvom pevnej siete a mobilného telefonického spojenia, prístupu na internet, internetovej elektronickej pošty, ako aj telefonovania prostredníctvom internetu a vzťahuje sa tak na všetky prostriedky elektronickej komunikácie, ktorých používanie je veľmi rozšírené v každodennom živote ľudí. Predstavuje teda zásah, ktorý ovplyvňuje celé európske obyvateľstvo. Vzhľadom na rozsah a závažnosť tohto zásahu by sa uchovávanie prevádzkových a lokalizačných údajov mohlo podľa SDEÚ odôvodniť len na účely boja proti závažnej trestnej činnosti. Okrem toho sa v smernici nestanovujú žiadne objektívne kritériá, ktoré by zabezpečili, že prístup príslušných vnútroštátnych orgánov k uchovávaným údajom je obmedzený na to, čo je nevyhnutne potrebné. Navyše smernica neobsahovala hmotnoprávne ani procesné podmienky upravujúce prístup k uchovávaným údajom a ich používanie vnútroštátnymi orgánmi, navyše prístup nepodliehal predchádzajúcej kontrole vykonanej buď súdom, alebo iným nezávislým orgánom.

SDEÚ dospel k podobnému záveru v spojených veciach *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.*⁶⁹. Tieto veci sa týkali uchovávania prevádzkových a lokalizačných údajov „všetkých účastníkov a registrovaných užívateľov a všetkých spôsobov elektronickej komunikácie, ako aj všetkých metaúdajov“ bez „rozlíšenia, obmedzenia alebo výnimky na základe sledovaného cieľa“.⁷⁰ V tomto prípade uchovávanie údajov osoby nebolo podmienené tým, či existovala priama alebo aspoň nepriama súvislosť medzi danou osobou a závažnou trestnou činnosťou, alebo či jej komunikácia bola alebo nebola relevantná pre národnú bezpečnosť. Vzhľadom na to, že neexistuje ani požadovaná súvislosť medzi

68 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014, bod 39.

69 SDEÚ, spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.* [VK], 21. decembra 2016, body 105 – 106.

70 Tamže, bod 105.

uchovávanými údajmi a hrozbou pre verejnú bezpečnosť, ani časové obmedzenie či obmedzenie zemepisnej oblasti, SDEÚ dospel k záveru, že táto vnútroštátna právna úprava prekračuje rámec toho, čo je prísne nevyhnutné na účely boja proti závažnej trestnej činnosti⁷¹.

Podobný prístup k nevyhnutnosti zastáva aj Európsky dozorný úradník pre ochranu údajov vo svojom súbore nástrojov s názvom *Necessity Toolkit*⁷². Tento súbor nástrojov má pomôcť pri posudzovaní súladu navrhovaných opatrení s právnymi predpismi EÚ o ochrane údajov. Bol vypracovaný s cieľom lepšie pripraviť tvorcov politik a zákonodarcov EÚ zodpovedných za prípravu alebo kontrolu opatrení, ktoré zahŕňajú spracúvanie osobných údajov a obmedzujú právo na ochranu osobných údajov a ďalšie práva a slobody stanovené v Charte.

Ciele všeobecného záujmu

Ak má byť akékoľvek obmedzenie výkonu práv uznaných v Charte odôvodnené, musí byť v skutočnom súlade aj s cieľmi všeobecného záujmu, ktoré sú uznané Úniou, alebo s potrebou ochrany práv a slobôd iných osôb. Pokiaľ ide o potrebu chrániť práva a slobody iných, často dochádza k vzájomnému pôsobeniu medzi právom na ochranu osobných údajov a inými základnými právami. V [oddiele 1.3](#) sa uvádza podrobná analýza takéhoto vzájomného pôsobenia. Pokiaľ ide o ciele všeobecného záujmu, tie zahŕňajú všeobecné ciele EÚ zakotvené v článku 3 Zmluvy o Európskej únii (ZEU), ako sú presadzovanie mieru a blaha jej národov, sociálna spravodlivosť a ochrana a vytvorenie priestoru slobody, bezpečnosti a spravodlivosti, v ktorom je zaručený voľný pohyb osôb, spolu s príslušnými opatreniami na predchádzanie trestnej činnosti a boja proti nej, ako aj iné ciele a záujmy chránené osobitnými ustanoveniami zmlúv⁷³. Vo všeobecnom nariadení o ochrane údajov sa v tejto súvislosti ďalej spresňuje článok 52 ods. 1 Charty: v článku 23 ods. 1 nariadenia sa uvádzajú ciele všeobecného záujmu, ktoré sa považujú za legitímne na účely obmedzenia práv jednotlivcov, pod podmienkou, že toto obmedzenie rešpektuje podstatu práva na ochranu osobných údajov a je nevyhnutné a primerané. K uvedeným cieľom verejného záujmu patrí národná bezpečnosť a obrana, predchádzanie trestným činom, ochrana dôležitých hospodárskych a finančných záujmov EÚ alebo členských štátov, verejné zdravie a sociálne zabezpečenie.

71 Tamže, bod 107.

72 EDPS (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017.

73 Vysvetlivky k Charte základných práv (2007/C 303/02), Ú. v. EÚ C 303, 2007, s. 17 – 35.

Je dôležité dostatočne podrobne vymedziť a vysvetliť cieľ všeobecného záujmu, ktorý sa obmedzením sleduje, keďže nevyhnutnosť obmedzenia sa bude posudzovať v jeho kontexte. Jasný a podrobný opis cieľa obmedzenia a navrhovaných opatrení je nevyhnutný na to, aby bolo možné posúdiť, či je nevyhnutné⁷⁴. Sledovaný cieľ a nevyhnutnosť a primeranosť obmedzenia spolu úzko súvisia.

Príklad: *Vec Schwarz/Stadt Bochum*⁷⁵ sa týkala obmedzenia práva na rešpektovanie súkromného života a práva na ochranu osobných údajov, ku ktorému dochádzalo pri odoberaní a uchovávaní odtlačkov prstov pri vydávaní cestovných pasov orgánmi členského štátu⁷⁶. Žalobca požiadal Stadt Bochum o vydanie cestovného pasu, nesúhlasil však s odobraním odtlačkov prstov; Stadt Bochum preto jeho žiadosť o vydanie cestovného pasu odmietlo. Následne podal žalobu na nemecký súd, v ktorej žiadal o vydanie cestovného pasu bez odobratia odtlačkov prstov. Nemecký súd postúpil vec SDEÚ, pričom mu položil otázku, či sa má článok 1 ods. 2 nariadenia č. 2252/2004 o normách pre bezpečnostné znaky a biometriu v pasoch a cestovných dokladoch vydávaných členskými štátmi považovať za platný.

SDEÚ poukázal na to, že odtlačky prstov **predstavujú osobné údaje**, keďže objektívne obsahujú jedinečné informácie o fyzických osobách a umožňujú ich presnú identifikáciu, pričom odoberanie a uchovávanie odtlačkov prstov predstavuje spracúvanie. Toto spracúvanie, na ktoré sa vzťahuje článok 1 ods. 2 nariadenia č. 2252/2004, predstavuje zásah do práva na rešpektovanie súkromného života a na ochranu osobných údajov⁷⁷. Podľa článku 52 ods. 1 Charty sa však pripúšťajú obmedzenia výkonu takýchto práv, pokiaľ sú tieto obmedzenia stanovené zákonom a rešpektujú podstatu týchto práv a ak sú – pri dodržaní zásady proporcionality – nevyhnutné a skutočne spĺňajú ciele všeobecného záujmu uznané Úniou alebo potrebu chrániť práva a slobody iných.

V tomto prípade SDEÚ najprv konštatoval, že obmedzenie, ktoré vyplýva z odoberania a ukladania odtlačkov prstov v rámci vydávania cestovných pasov, treba považovať za **stanovené zákonom**, keďže v článku 1 ods. 2 nariadenia č. 2252/2004 sa stanovujú tieto úkony. Po druhé bolo cieľom

74 EDPS (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017, s. 4.

75 SDEÚ, C-291/12, *Michael Schwarz/Stadt Bochum*, 17. októbra 2013.

76 Tamže, body 33 – 36.

77 Tamže, body 27 – 30.

tohto nariadenia predchádzať falšovaniu cestovných pasov a zabrániť ich podvodnému používaniu. Článkom 1 ods. 2 sa teda sleduje cieľ zabrániť, okrem iného, nezákonnému vstupu do EÚ, a tak sa sleduje cieľ všeobecného záujmu uznaný Úniou. Po tretie z údajov, ktorými disponuje SDEÚ, nevyplýva a navyše sa ani neuvádzalo, že obmedzenia stanovené v danom prípade na výkon práv nerešpektujú podstatu týchto práv. Po štvrté si ukladanie odtlačkov prstov na vysoko zabezpečené pamäťové médium stanovené v tomto ustanovení vyžaduje sofistikovanú techniku. Toto ukladanie pravdepodobne zníži nebezpečenstvo falšovania cestovných pasov a uľahčí úlohu orgánov poverených skúmaním ich pravosti na hraniciach EÚ. Skutočnosť, že uvedená metóda nie je úplne spoľahlivá, nie je rozhodujúca. Hoci táto metóda nevylučuje akceptáciu neoprávnených osôb, postačuje na to, aby podstatne znížila nebezpečenstvo takýchto akceptácií. Vzhľadom na vyššie uvedené úvahy SDEÚ konštatoval, že odoberanie a ukladanie odtlačkov prstov uvádzané v článku 1 ods. 2 nariadenia č. 2252/2004 je primerané na dosiahnutie cieľov, ktoré sa týmto nariadením sledujú, a teda aj cieľa zabrániť nelegálnemu vstupu osôb na územie Únie⁷⁸.

SDEÚ sa ďalej zaoberal tým, či je takéto spracúvanie **nevyhnutné**, pričom konštatoval, že predmetné opatrenie spočíva iba v odobratí odtlačkov dvoch prstov, pričom prsty sú obvykle vystavené pohľadu iných osôb, takže nejde o úkon intímneho charakteru. Tento úkon sa nespája ani s osobitnými fyzickými alebo psychickými ťažkosťami pre dotknutú osobu, podobne ako nasnímanie fotografie tváre. Takisto treba poznamenať, že jediná reálna alternatíva odoberania odtlačkov prstov spomínaná v priebehu konania pred SDEÚ spočívala v nasnímaní obrazu očnej dúhovky. Nič v spise predloženom SDEÚ pritom nenasvedčuje, že tento postup by do práv priznaných článkami 7 a 8 Charty zasahoval menej než odoberanie odtlačkov prstov. Okrem toho, pokiaľ ide o efektívnosť týchto dvoch metód, je nesporné, že úroveň technologickej vyspelosti metódy založenej na rozpoznávaní očnej dúhovky nedosahuje úroveň metódy založenej na odtlačkoch prstov. Navyše rozpoznávanie očnej dúhovky je zatiaľ podstatne drahším postupom než postup porovnania odtlačkov prstov, a preto je menej vhodný na všeobecné používanie. SDEÚ navyše nebol informovaný o existencii žiadnych opatrení, ktoré by mohli dostatočne účinne prispievať k cieľu spočívajúcemu v ochrane cestovných

78 Tamže, body 35 – 45.

pasov pred ich podvodným používaním, ale zároveň by spôsobovali menší zásah do práv priznaných článkami 7 a 8 Charty než zásah, ktorý predstavuje metóda založená na odtlačkoch prstov⁷⁹.

SDEÚ konštatoval, že v článku 4 ods. 3 nariadenia č. 2252/2004 sa výslovne uvádza, že odtlačky prstov sa môžu používať iba na účel overovania pravosti cestovného pasu a totožnosti jeho držiteľa, pričom v článku 1 ods. 2 nariadenia sa stanovuje uchovávanie odtlačkov prstov iba v samotnom cestovnom pase, ktorý zostáva vo výlučnej držbe jeho držiteľa. Nariadenie teda neposkytlo právny základ pre centralizované uchovávanie údajov získaných na jeho základe ani na použitie týchto údajov na iné účely než zabránenie nelegálnemu vstupu osôb na územie Únie⁸⁰. Vzhľadom na všetky predchádzajúce úvahy SDEÚ dospel k záveru, že preskúmaním položenej otázky sa neodhalila žiadna skutočnosť, ktorá by mohla mať vplyv na platnosť článku 1 ods. 2 nariadenia č. 2252/2004.

Vzťah medzi Chartou a ECHR

Napriek odlišnému zneniu podmienky zákonného obmedzenia práv, ktoré je uvedené v článku 52 ods. 1 Charty, pripomína znenie článku 8 ods. 2 ECHR, ktoré sa týka práva na rešpektovanie súkromného života. SDEÚ a ESLP sa vo svojich judikaturách často navzájom odvolávajú na svoje rozsudky v rámci stáleho dialógu medzi oboma súdmi s cieľom dosiahnuť harmonický výklad pravidiel ochrany údajov. V článku 52 ods. 3 Charty sa stanovuje, že „v rozsahu, v akom táto Charta obsahuje práva, ktoré zodpovedajú právam zaručeným v Európskom dohovore o ochrane ľudských práv a základných slobôd, zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom Dohovore“. Článok 8 Charty však nezodpovedá priamo konkrétnemu článku ECHR⁸¹. Článok 52 ods. 3 Charty sa týka obsahu a rozsahu práv chránených oboma právnymi poriadkami, nie však podmienok ich obmedzenia. Vzhľadom na širší kontext dialógu a spolupráce medzi týmito dvoma súdmi môže SDEÚ vo svojich analýzach zohľadniť kritériá zákonného obmedzenia podľa článku 8 ECHR, vo výklade ESLP. Do úvahy prichádza aj opačný scenár, podľa ktorého ESLP môže odkazovať na podmienky zákonného obmedzenia podľa Charty. V každom prípade by sa však malo zohľadniť, že v ECHR neexistuje dokonalý ekvivalent článku 8 Charty, ktorý by sa týkal ochrany osobných údajov, a najmä práv

79 SDEÚ, C-291/12, *Michael Schwarz/Stadt Bochum*, 17. októbra 2013, body 46 – 53.

80 Tamže, body 56 – 61.

81 EDPS (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017, s. 6.

dotknutej osoby, legitímnych základov na spracúvanie a dohľadu nezávislým orgánom. Niektoré prvky článku 8 Charty môžu vychádzať z judikatúry ESĽP vypracovanej na základe článku 8 ECHR a v súvislosti s Dohovorom č. 108⁸². Táto súvislosť zabezpečuje existenciu vzájomnej inšpirácie medzi SDEÚ a ESĽP vo veciach týkajúcich sa ochrany údajov.

1.3. Vzájomné pôsobenie vo vzťahu k iným právam a oprávneným záujmom

Hlavné body

- Právo na ochranu údajov sa často vzájomne ovplyvňuje s inými právami, ako je sloboda prejavu a právo prijímať a rozširovať informácie.
- Toto vzájomné pôsobenie je často nejednoznačné: hoci existujú situácie, keď je právo na ochranu osobných údajov v konflikte s konkrétnym právom, existujú aj situácie, keď právo na ochranu osobných údajov účinne zabezpečuje dodržiavanie práve daného konkrétneho práva. Platí to napríklad v prípade slobody prejavu, keďže služobné tajomstvo je súčasťou práva na rešpektovanie súkromného života.
- Potreba ochrany práv a slobôd iných je jedným z kritérií na posúdenie zákonného obmedzenia práva na ochranu osobných údajov.
- Ak sú ohrozené rôzne práva, súdy sa musia usilovať o ich vzájomné vyváženie a zosúladienie.
- Vo všeobecnom nariadení o ochrane údajov sa od členských štátov vyžaduje, aby zosúladiť právo na ochranu osobných údajov s právom na slobodu prejavu a informácie.
- Členské štáty môžu takisto prijať osobitné vnútroštátne predpisy s cieľom zosúladiť právo na ochranu osobných údajov s prístupom verejnosti k úradným dokumentom a povinnosťou služobného tajomstva.

Právo na ochranu osobných údajov nie je absolútne právo a podmienky jeho zákonného obmedzenia už boli opísané vyššie. Jedným z kritérií zákonných obmedzení práv, ktoré sa uznávajú v rámci práva RE, ako aj práva EÚ je, že zásah do ochrany údajov je nevyhnutný na ochranu práv a slobôd iných. Ak pri ochrane údajov dochádza k vzájomnému ovplyvňovaniu s inými právami, ESĽP aj SDEÚ opakovane

82 Vysvetlivky k európskej Charte základných práv 2007/C 303/02, článok 8.

konštatujú, že pri uplatňovaní a výklade článku 8 ECHR a článku 8 Charty je potrebné vyvažovať toto právo s ostatnými právami⁸³. Na niekoľkých príkladoch si ukážeme, ako sa takáto rovnováha dosahuje.

Okrem vzájomného vyvažovania, ktoré vykonávajú súdy, môžu štáty v prípade potreby prijať právne predpisy na zosúladienie práva na ochranu osobných údajov s inými právami. Z tohto dôvodu sa vo všeobecnom nariadení o ochrane údajov uvádza niekoľko oblastí, v ktorých je možná vnútroštátna výnimka.

Pokiaľ ide o slobodu prejavu, podľa GDPR sa od členských štátov vyžaduje, že právnymi predpismi „zosúladia právo na ochranu osobných údajov podľa tohto nariadenia s právom na slobodu prejavu a právom na informácie vrátane spracúvania na žurnalistické účely a na účely akademickej, umeleckej alebo literárnej tvorby“⁸⁴. Členské štáty môžu okrem toho prijať právne predpisy na zosúladienie ochrany údajov s prístupom verejnosti k úradným dokumentom a povinnosťou služobného tajomstva, ktoré sú chránené ako určitá forma práva na rešpektovanie súkromného života⁸⁵.

1.3.1. Sloboda prejavu

Jedným z práv, ktoré sa s právom na ochranu údajov najviac navzájom ovplyvňujú, je právo na slobodu prejavu.

Sloboda prejavu je chránená článkom 11 Charty (Sloboda prejavu a právo na informácie). Toto právo zahŕňa „slobodu zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice“. Právo na informácie chráni podľa článku 11 Charty a článku 10 ECHR nielen právo rozširovať informácie, ale aj právo *prijímať* informácie.

Obmedzenia slobody prejavu musia byť v súlade s kritériami uvedenými v článku 52 ods. 1 Charty, ktoré sú opísané vyššie. Okrem toho článok 11 Charty zodpovedá článku 10 ECHR. Podľa článku 52 ods. 3 Charty, v rozsahu, v akom obsahuje práva, ktoré zodpovedajú právam zaručeným v ECHR, „zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom Dohovore.“ Obmedzenia,

83 ESJP, *Von Hannover/Nemecko* (č. 2) [VK], č. 40660/08 a 60641/08, 7. februára 2012; SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEDM)/Administración del Estado*, 24. novembra 2011, bod 48; SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [VK], 29. januára 2008, bod 68.

84 Všeobecné nariadenie o ochrane údajov, článok 85.

85 Tamže, článok 86 a 90.

ktoré môžu byť zo zákona uložené na právo zaručené článkom 11 Charty, teda nesmú byť rozsiahlejšie ako obmedzenia stanovené v článku 10 ods. 2 ECHR, čo znamená, že musia byť predpísané zákonom a musia byť nevyhnutné v demokratickej spoločnosti „na ochranu [...] povesti alebo práv iných“. Takéto práva zahŕňajú najmä právo na rešpektovanie súkromného života a právo na ochranu osobných údajov.

Vzťah medzi ochranou osobných údajov a slobodou prejavu je upravený článkom 85 všeobecného nariadenia o ochrane údajov s názvom „Spracúvanie a sloboda prejavu a právo na informácie“. Podľa tohto článku členské štáty zosúladiť právo na ochranu osobných údajov s právom na slobodu prejavu a právom na informácie. Výnimky a odchýlky z ustanovení konkrétnych kapitol všeobecného nariadenia o ochrane údajov sú možné na žurnalistické účely alebo účely akademickej, umeleckej alebo literárnej tvorby, iba vtedy, ak sú potrebné na zosúladenie práva na ochranu osobných údajov so slobodou prejavu a právom na informácie.

Príklad: SDEÚ bol vo veci *Tietosuojavaluutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy*⁸⁶ požiadaný o vymedzenie vzťahu medzi ochranou údajov a slobodou tlače⁸⁷. Zaoberal sa spoločnosťou, ktorá šírla údaje o daniach približne 1,2 milióna fyzických osôb prostredníctvom služby zasielania SMS, pričom uvedené údaje boli zákonným spôsobom získané od fínskych daňových orgánov. Fínsky dozorný orgán pre ochranu údajov vydal rozhodnutie, v ktorom od spoločnosti požaduje, aby zastavila šírenie týchto údajov. Spoločnosť napadla toto rozhodnutie na vnútroštátnom súde, ktorý požiadal SDEÚ o objasnenie výkladu smernice o ochrane údajov. SDEÚ musel predovšetkým preskúmať, či treba spracúvanie osobných údajov, ktoré daňové orgány sprístupnili s cieľom umožniť používateľom mobilných telefónov získavať údaje o daniach týkajúce sa iných fyzických osôb, považovať za činnosť vykonávanú výlučne na žurnalistické účely. SDEÚ dospel k záveru, že činnosť spoločnosti predstavuje „spracúvanie osobných údajov“ v zmysle článku 3 ods. 1 smernice o ochrane údajov, a pokračoval výkladom článku 9 uvedenej smernice (o spracúvaní osobných údajov a slobode prejavu). Najskôr poukázal na význam práva na slobodu prejavu v každej demokratickej spoločnosti a uviedol, že

86 SDEÚ, C-73/07, *Tietosuojavaluutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy* [VK], 16. decembra 2008, body 56, 61 a 62.

87 Vec sa týkala výkladu článku 9 smernice o ochrane údajov, v súčasnosti nahradeného článkom 85 všeobecného nariadenia o ochrane údajov, ktorý znie: „Členské štáty vykonajú opatrenia pre výnimky a odchýlky z ustanovení tejto kapitoly, kapitoly IV a kapitoly VI pre spracovanie osobných údajov, vykonávané výlučne na žurnalistické účely alebo účely umeleckého alebo literárneho vyjadrenia, iba vtedy, ak sú nevyhnutné pre uvedenie práva na súkromie do súladu s nariadeniami, ktorými sa riadi sloboda prejavu.“

pojmy súvisiace s touto slobodou, napríklad žurnalistika, si vyžadujú širokú interpretáciu. Následne konštatoval, že v záujme dosiahnutia rovnováhy medzi týmito dvoma základnými právami sa výnimky a obmedzenia práva na ochranu údajov musia uplatňovať len do tej miery, do akej sú nevyhnutne potrebné. Za uvedených okolností SDEÚ dospel k záveru, že činnosti, ktoré vykonávala predmetná spoločnosť, týkajúce sa údajov z dokumentov, ktoré sú podľa vnútroštátnych právnych predpisov verejne dostupné, možno klasifikovať ako „žurnalistické činnosti“ vtedy, keď je ich cieľom zverejnenie informácií, názorov alebo myšlienok, a to bez ohľadu na médium použité na ich poskytnutie. Súd takisto konštatoval, že tieto činnosti sa neobmedzujú na médiá a môžu sa vykonávať na účely dosahovania zisku. Rozhodnutie o skutkových okolnostiach tohto konkrétneho prípadu však SDEÚ ponechal na vnútroštátnom súde.

Túto vec preskúmal aj ESLP po tom, ako vnútroštátny súd na základe usmerenia SDEÚ rozhodol, že rozhodnutie dozorného orgánu zastaviť zverejňovanie všetkých daňových informácií predstavuje odôvodnený zásah do slobody prejavu danej spoločnosti. ESLP tento výklad potvrdil⁸⁸. Konštatoval, že hoci došlo k zásahu do práva spoločnosti na šírenie informácií, zásah bol v súlade s právnymi predpismi, sledoval legitímny cieľ a bol nevyhnutný v demokratickej spoločnosti.

Súd pripomenul kritériá judikatúry, ktorými by sa mali riadiť vnútroštátne orgány a samotný ESLP pri hľadaní rovnováhy medzi slobodou prejavu a právom na rešpektovanie súkromného života. Ak ide o politický prejav alebo diskusiu o otázkach verejného záujmu, existuje len obmedzený priestor na obmedzenie práva prijímať a rozširovať informácie, keďže verejnosť má právo byť informovaná, „a ide o základné právo v demokratickej spoločnosti“⁸⁹. Články v tlači, ktorých jediným cieľom je uspokojiť záujem určitého okruhu čitateľov, pokiaľ ide o podrobnosti o súkromnom živote určitej osoby, však nemožno považovať za príspevok k diskusii vo verejnom záujme. Cieľom výnimky z pravidiel ochrany údajov na žurnalistické účely je umožniť novinárom získať prístup k údajom, zbierať ich a spracúvať, aby mohli vykonávať svoje žurnalistické činnosti. Preto skutočne existoval verejný záujem na tom, aby sa sťažujúcim sa spoločnostiam poskytla možnosť získavať a spracúvať spomínané veľké objemy daňových údajov. ESLP naopak konštatoval, že neexistuje verejný záujem na hromadnom šírení takýchto nespracúvaných

88 ESLP, *Satakunnan Markkinapörssi Oy a Satamedia Oy/Fínsko*, č. 931/13, 27. júna 2017.

89 Tamže, bod 169.

údajov ich uverejnením v novinách v nezmenenej podobe a bez akejkoľvek analýzy. Tieto daňové informácie mohli zvedavým príslušníkom verejnosti umožniť, aby kategorizovali ľudí podľa ich ekonomického postavenia, a uspokojili by tak záujem verejnosti o informácie o súkromnom živote iných osôb. Nemožno to však považovať za príspevok k diskusii vo verejnom záujme.

Príklad: Vo veci *Google Spain*⁹⁰ sa SDEÚ zaoberal otázkou, či je spoločnosť Google povinná vymazať neaktuálne informácie o finančných ťažkostiach žalobcu zo svojho zoznamu výsledkov vyhľadávania. Po vyhľadávaní uskuutočnenom na základe zadania mena žalobcu sa vo výsledkoch vyhľadávania zobrazili odkazy na staré novinové články, v ktorých sa spomínal v súvislosti s konkurzným konaním. Žalobca sa domnieva, že ide o porušenie práv na rešpektovanie súkromného života a na ochranu osobných údajov, keďže toto konanie bolo ukončené už dávno a tieto odkazy sú teda irelevantné.

SDEÚ najprv objasnil, že internetové vyhľadávače a výsledky vyhľadávania, ktoré obsahujú osobné údaje, umožňujú vytvorenie podrobného profilu jednotlivca. Vzhľadom na čoraz väčšiu digitalizáciu spoločnosti je požiadavka, aby osobné údaje boli správne a aby ich uverejnenie neprekračovalo rámec toho, čo je nevyhnutné, t. j. poskytovať verejnosti informácie, základnou požiadavkou pri zabezpečovaní vysokej úrovne ochrany údajov pre jednotlivcov. „Prevádzkovateľ tohto spracovania musí v rámci svojich zodpovedností, kompetencií a možností zaručiť, že toto spracovanie spĺňa požiadavky“ práva Únie, aby záruky ňou stanovené mohli mať plný účinok. To znamená, že právo na vymazanie osobných údajov v prípade, že spracúvanie už nie je potrebné alebo je neaktuálne, sa vzťahuje aj na vyhľadávače, ktoré sa považujú za prevádzkovateľov, a nie len za sprostredkovateľov (pozri [oddiel 2.3.1](#)).

Pri skúmaní toho, či bola spoločnosť Google povinná odstrániť odkazy týkajúce sa žalobcu, SDEÚ rozhodol, že jednotlivci majú za určitých podmienok právo požadovať výmaz svojich osobných údajov z výsledkov vyhľadávania internetového vyhľadávača. Toto právo sa môže uplatniť v prípade, že informácie týkajúce sa určitej osoby sú nepresné, neadekvátne, irelevantné alebo neprimerané na účely spracúvania údajov. SDEÚ uznal, že toto právo nie je absolútne; musí byť v rovnováhe s inými právami, najmä s ohľadom na záujem a právo širokej verejnosti na prístup k informáciám. Pri každej žiadosti o výmaz sa vyžaduje individuálne posúdenie s cieľom nájsť rovnováhu medzi

90 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, body 81 – 83.

základnými právami na ochranu osobných údajov a ochranu súkromného života dotknutej osoby na jednej strane a oprávnenými záujmami všetkých používateľov internetu na strane druhej. SDEÚ poskytol usmernenia k faktorom, ktoré by sa mali pri hľadaní tejto rovnováhy zohľadňovať. Mimoriadne dôležitým faktorom je povaha predmetných informácií. Ak sú informácie citlivé pre súkromný život jednotlivca a ak neexistuje verejný záujem na dostupnosti týchto informácií, ochrana údajov a súkromia by mala prevažovať nad právom širokej verejnosti na prístup k informáciám. Naopak, ak je zrejmé, že dotknutá osoba je verejne činná osoba, alebo že tieto informácie sú takej povahy, ktorá by odôvodňovala, aby sa k nim poskytol prístup širokej verejnosti, potom je zásah do základných práv na ochranu údajov a súkromia odôvodnený.

V nadväznosti na tento rozsudok SDEÚ prijala pracovná skupina zriadená podľa článku 29 usmernenia o jeho vykonávaní. Usmernenia obsahujú zoznam spoločných kritérií, ktoré majú uplatňovať dozorné orgány pri vybavovaní sťažností týkajúcich sa žiadostí jednotlivcov o vymazanie a ktoré ich majú usmerňovať pri tomto porovnávacom teste⁹¹.

ESLP vyniesol viacero prelomových rozsudkov týkajúcich sa o zosúladenia práva na ochranu údajov s právom na slobodu prejavu.

Príklad: Vo veci *Axel Springer AG/Nemecko*⁹² ESLP dospel k záveru, že súdny príkaz ukladajúci povinnosť zdržať sa určitého konania, uložený sťažujúcej sa spoločnosti, ktorá chcela uverejniť článok o uväznení a odsúdení známeho herca, predstavuje porušenie článku 10 ECHR. ESLP pripomenul kritériá, ktoré stanovil vo svojej judikatúre, pokiaľ ide o vyváženie práva na slobodu prejavu s právom na rešpektovanie súkromného života:

- či udalosť, ktorej sa týkal uverejnený článok, bola vo všeobecnom záujme,
- či dotknutá osoba bola verejne činnou osobou a
- akým spôsobom boli informácie získané a či boli spoľahlivé.

91 Pracovná skupina zriadená podľa článku 29 (2014), *Usmernenia o vykonávaní rozsudku Súdneho dvora Európskej únie vo veci „Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Marioivi Costejovi Gonzálezovi“ C-131/12*, WP 225, Brusel, 26. novembra 2014.

92 ESLP, *Axel Springer AG/Nemecko* [VK], č. 39954/08, 7. februára 2012, body 90 a 91.

ESLP dospel k záveru, že uväznenie a odsúdenie herca predstavovalo verejnú súdnu skutočnosť, išlo teda o verejný záujem; herec bol dostatočne známy na to, aby sa mohol považovať za verejne činnú osobu; informácie poskytla kancelária prokurátora a strany nespochybnili presnosť informácií. Obmedzenie uverejnenia, ktoré bolo spoločnosti uložené, preto nebolo primerané legitímnemu cieľu ochrany súkromného života žalobcu. Súd dospel k záveru, že došlo k porušeniu článku 10 ECHR.

Príklad: *Vec Couderc a Hachette Filipacchi Associés/Francúzsko*⁹³ sa týkala uverejnenia rozhovoru vo francúzskom týždenníku s pani Coste, ktorá tvrdila, že monacké knieža Albert je otcom jej syna. V rozhovore bol opísaný aj vzťah pani Coste s kniežaťom a to, ako reagoval na narodenie dieťaťa, spolu s fotografiami kniežaťa s dieťaťom. Knieža Albert podal žalobu proti vydavateľskej spoločnosti vo veci porušenia jeho práva na ochranu súkromného života. Francúzske sudy konštatovali, že uverejnenie tohto článku spôsobilo kniežaťu Albertovi nenapraviteľnú škodu, a uložili vydavateľstvu povinnosť škodu nahradiť a uverejniť informácie o rozsudku na titulnej strane časopisu.

Vydavatelia časopisu sa obrátili na ESLP s tvrdením, že rozsudok francúzskych súdov neoprávnene zasahoval do ich práva na slobodu prejavu. ESLP musel vyvážiť právo na rešpektovanie súkromného života kniežaťa Alberta s právom vydavateľa na slobodu prejavu a právom širokej verejnosti na informácie. Rovnako dôležité bolo aj zohľadniť právo pani Coste podeliť sa o svoj príbeh s verejnosťou a záujem dieťaťa na oficiálnom potvrdení vzťahu s otcom.

ESLP rozhodol, že zverejnenie rozhovoru predstavuje zásah do súkromného života kniežaťa, a následne preskúmal, či bol zásah nevyhnutný. Dospel k záveru, že zverejnenie sa týkalo verejného činiteľa a záležitosti verejného záujmu, keďže občania Monaka mali záujem byť informovaní o existencii dieťaťa kniežaťa, keďže budúcnosť dedičnej monarchie je „neoddeliteľne spojená s existenciou potomkov“, a teda je predmetom záujmu verejnosti⁹⁴. Súd tiež konštatoval, že tento článok umožnil pani Coste a jej dieťaťu uplatniť ich právo na slobodu prejavu. Vnútroštátne sudy náležite nezohľadnili zásady a kritériá

93 ESLP, *Couderc a Hachette Filipacchi Associés/Francúzsko*[VK], č. 40454/07, 10. novembra 2015.

94 Tamže, body 104 – 116.

stanovené v judikatúre ESĽP týkajúce sa vyváženia práva na rešpektovanie súkromného života s právom na slobodu prejavu. Súd dospel k záveru, že Francúzsko porušilo článok 10 ECHR o slobode prejavu.

V judikatúre ESĽP je jedným z rozhodujúcich kritérií vyváženia týchto práv to, či predmetný prejav prispieva k diskusii vo všeobecnom verejnom záujme alebo nie.

Príklad: Vo veci *Mosley/Spojené kráľovstvo*⁹⁵ celoštátny týždenník uverejnil intímne fotografie sťažovateľa, známej osobnosti, ktorá následne úspešne žalovala vydavateľa a získala náhradu škody. Napriek priznanej peňažnej náhrade škody sa sťažovateľ sťažoval, že sa naďalej porušuje jeho právo na súkromie, keďže nemohol požiadať o vydanie súdneho príkazu pred uverejnením predmetných fotografií, keďže na noviny sa nevzťahuje žiadna zákonná požiadavka, aby uverejnenie vopred oznámili.

ESĽP konštatoval, že aj keď účelom šírenia takéhoto materiálu bola vo všeobecnosti skôr zábava než vzdelávanie, nepochybne sa naň vzťahuje ochrana vyplývajúca z článku 10 ECHR, ktorý sa môže oprieť o požiadavky článku 8 ECHR, ak ide o informácie súkromnej a intímnej povahy, pri ktorých neexistuje žiadny verejný záujem na ich šírení. Zvlášť opatrne treba postupovať pri skúmaní obmedzení, ktoré by mohli pôsobiť ako forma cenzúry pred uverejnením. Pokiaľ ide o odstrašujúci účinok, ktorý by mohla mať požiadavka predbežného oznamovania, pochybnosti o jej účinnosti a súvisiaci široký priestor na voľnú úvahu, ESĽP dospel k záveru, že podľa článku 8 sa nevyžaduje povinnosť právne záväznej požiadavky predbežného oznamovania. Súd preto skonštatoval, že nedošlo k porušeniu článku 8.

Príklad: Vo veci *Bohlen/Nemecko*⁹⁶ sťažovateľ, známy spevák a umelecký producent, vydal autobiografickú knihu a následne bol na základe súdnych rozhodnutí nútený z nej niektoré časti odstrániť. Celoštátne médiá tejto záležitosti venovali značnú pozornosť a istá tabaková spoločnosť začala vtipnú reklamnú kampaň, ktorá na túto udalosť odkazovala a v ktorej bolo použité krstné meno sťažovateľa bez jeho súhlasu. Sťažovateľ sa neúspešne snažil získať náhradu škody od príslušnej reklamnej spoločnosti na základe tvrdenia, že ide o porušenie jeho práv podľa článku 8 ECHR. ESĽP potvrdil kritériá, na

95 ESĽP, *Mosley/Spojené kráľovstvo*, č. 48009/08, 10. mája 2011, body 129 a 130.

96 ESĽP, *Bohlen/Nemecko*, č. 53495/09, 19. februára 2015, body 45 – 60.

základe ktorých sa vyvažuje právo na rešpektovanie súkromného života s právom na slobodu prejavu, a dospel k záveru, že nedošlo k porušeniu článku 8. Sťažovateľ bol verejne známou osobnosťou a reklama neodkazovala na informácie o jeho súkromnom živote, ale na verejnú udalosť, ktorej už bola venovaná pozornosť v médiách a ktorá bola súčasťou verejnej diskusie. Okrem toho mala reklama vtipný podtón a sťažovateľa žiadnym spôsobom neponižovala ani nestavala do negatívneho svetla.

Príklad: Vo veci *Biriuk/Litva*⁹⁷ sťažovateľka pred ESLP tvrdila, že Litva si nespĺnila povinnosť zabezpečiť rešpektovanie jej práva na súkromný život, pretože aj napriek tomu, že významný denník závažne porušil jej súkromie, vnútroštátne súdy, ktoré tento prípad vyšetrovali, jej priznali finančné odškodnenie len v nepatrnej sume. Pri rozhodovaní o priznaní náhrady za nemajetkovú ujmu vnútroštátne súdy uplatnili vnútroštátne právne predpisy týkajúce sa poskytovania informácií verejnosti, v ktorých je stanovený nízky strop náhrady za nemajetkovú ujmu spôsobenú protiprávnym verejným šírením informácií o súkromnom živote prostredníctvom médií. Podstatou veci bola skutočnosť, že najväčší litovský denník na svojej titulnej strane uverejnil článok, v ktorom sa uvádza, že sťažovateľka je HIV pozitívna. V článku sa tiež kritizovalo správanie sťažovateľky a spochybňovali jej morálne zásady.

ESLP pripomenul, že ochrana osobných údajov, a najmä zdravotných údajov, má zásadný význam pri uplatňovaní práva jednotlivca na rešpektovanie súkromného života podľa ECHR. Dôvernoscť údajov týkajúcich sa zdravia je mimoriadne dôležitá, keďže zverejnenie zdravotných údajov (v tomto prípade nakazenie sťažovateľky HIV) môže dramaticky ovplyvniť súkromný a rodinný život danej osoby, jej situáciu v zamestnaní a začlenenie do spoločnosti. Sú osobitne zdôraznil skutočnosť, že podľa novinovej správy poskytol informácie o nákaze sťažovateľky vírusom HIV zdravotnícky personál nemocnice, a to v zjavnom rozpore s povinnosťou zachovávať lekárske tajomstvo. Nešlo teda o oprávnený zásah do práva sťažovateľky na súkromný život.

Článok bol však uverejnený v tlači a sloboda prejavu je tiež základným právom podľa ECHR. Pri preskúmaní otázky, či existencia verejného záujmu odôvodňuje zverejnenie tohto druhu informácií o sťažovateľke, ESLP konštatoval, že hlavným cieľom zverejnenia bolo zvýšiť predaj novín uspokojením zvedavosti čitateľov. ESLP sa nedomnieval, že by predmetný článok prispel

97 ESLP, *Biriuk/Litva*, č. 23373/03, 25. novembra 2008.

k akejkoľvek diskusii vo všeobecnom záujme spoločnosti. Vzhľadom na to, že išlo o „poburujúce zneužitie slobody tlače“, výrazné obmedzenia pri náprave škody a nízka suma náhrady za nemajetkovú ujmu podľa vnútroštátneho práva znamenali, že Litva nesplnila svoju pozitívnu povinnosť chrániť právo sťažovateľky na súkromný život. ESLP dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Právo na slobodu prejavu a právo na ochranu osobných údajov nie sú vždy v konflikte. Existujú prípady, keď účinná ochrana osobných údajov zaručuje slobodu prejavu.

Príklad: SDEÚ vo veci *Tele2 Sverige* konštatoval, že zásah spôsobený smernicou 2006/24 (smernica o uchovávaní údajov) do základných práv stanovených v článkoch 7 a 8 Charty bol „rozsiahly a treba ho považovať za zvlášť závažný. Okrem toho okolnosť, že uchovávanie údajov a ich neskoršie použitie bez toho, aby účastník alebo registrovaný užívateľ boli o tom informovaní, môže v povedomí dotknutých osôb vyvolať pocit, že ich súkromný život je predmetom neustáleho sledovania“. SDEÚ ďalej dospel k záveru, že takéto všeobecné uchovávanie prevádzkových a lokalizačných údajov môže mať vplyv na používanie elektronických komunikačných prostriedkov, a „v dôsledku toho na výkon slobody prejavu zaručenej v článku 11 Charty používateľmi týchto elektronických prostriedkov“⁹⁸. V tomto zmysle pravidlá ochrany údajov v konečnom dôsledku prispievajú k uplatňovaniu slobody prejavu tým, že vyžadujú, aby sa prísne záruky pri uchovávaní údajov neuplatňovali všeobecne.

Pokiaľ ide o právo prijímať informácie, ktoré je takisto súčasťou slobody prejavu, narastá význam transparentnosti štátnej správy pre fungovanie demokratickej spoločnosti. Transparentnosť je cieľom všeobecného záujmu, ktorý by v prípade potreby mohol odôvodňovať zásah do práva na ochranu údajov, ak je to nevyhnutné a primerané podľa [oddielu 1.2](#). V uplynulých dvoch desaťročiach bol preto uznaný význam práva na prístup k dokumentom, ktoré uchovávajú orgány verejnej moci, ako

⁹⁸ SDEÚ, spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.* [VK], 21. decembra 2016, bod 101; SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014, bod 28.

dôležitého práva každého občana EÚ a každej fyzickej alebo právnickej osoby, ktorá má pobyt alebo sídlo v niektorom členskom štáte.

V rámci právnych predpisov RE možno odkázať na zásady zakotvené v odporúčaní o prístupe k úradným dokumentom, ktorými sa inšpirovali autori Dohovoru o prístupe k úradným dokumentom (Dohovor č. 205)⁹⁹.

V rámci právnych predpisov EÚ je právo na prístup k dokumentom zaručené nariadením č. 1049/2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (nariadenie o prístupe k dokumentom)¹⁰⁰. Toto právo bolo rozšírené článkom 42 Charty a článkom 15 ods. 3 ZFEÚ na prístup „k dokumentom inštitúcií, orgánov, úradov a agentúr Únie bez ohľadu na ich nosič“.

Toto právo by sa mohlo dostať do konfliktu s právom na ochranu údajov v prípade, ak by sa sprístupnením dokumentov zverejnili osobné údaje iných osôb. V článku 86 všeobecného nariadenia o ochrane údajov sa jasne stanovuje, že osobné údaje v úradných dokumentoch, ktoré má v držbe orgán verejnej moci alebo verejnoprávny subjekt, môže daný orgán alebo subjekt poskytnúť v súlade s právom Únie¹⁰¹ alebo právom členského štátu, s cieľom zosúladiť prístup verejnosti k úradným dokumentom s právom na ochranu osobných údajov podľa tohto nariadenia.

Preto je potrebné vyvážiť žiadosti o prístup k dokumentom alebo informáciám uchovávaným verejnými orgánmi s právom na ochranu údajov osôb, ktorých údaje sú obsiahnuté v požadovaných dokumentoch.

Príklad: SDEÚ musel vo veci *Volker a Markus Schecke a Hartmut Eifert/Land Hessen*¹⁰² rozhodnúť o primeranosti uverejnenia mien príjemcov poľnohospodárskych dotácií EÚ a prijatých súm, ktoré sa požadovalo v právnych predpisoch EÚ. Cieľom zverejnenia bolo zvýšiť transparentnosť a prispieť k verejnej kontrole primeraného využívania verejných finančných prostriedkov verejnou správou. Viacero príjemcov spochybnilo primeranosť tohto zverejnenia.

99 Rada Európy, Výbor ministrov (2002), Odporúčanie R (81)219 a Odporúčanie Rec(2002)2 členským štátom o prístupe k oficiálnym dokumentom, 21. februára 2002; Rada Európy, Dohovor o prístupe k úradným dokumentom, CETS č. 205, 18. júna 2009. Dohovor zatiaľ nenadobudol účinnosť.

100 Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie, Ú. v. ES L 145, 2001.

101 Článok 42 Charty, článok 15 ods. 3 ZFEÚ a nariadenie č. 1049/2009.

102 SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010, body 47 – 52, 58, 66 – 67, 75, 86 a 92.

SDEÚ poznamenal, že právo na ochranu údajov nie je absolútne, a tvrdil, že uverejnenie údajov obsahujúcich mená príjemcov finančných prostriedkov z dvoch fondov poľnohospodárskej pomoci EÚ a presných súm, ktoré prijali, na webovom sídle, predstavuje všeobecný zásah do ich súkromného života a konkrétny zásah do ochrany ich osobných údajov.

SDEÚ konštatoval, že takéto porušenie článkov 7 a 8 Charty bolo stanovené zákonom a sledovalo cieľ všeobecného záujmu uznaného EÚ, a to konkrétne zvýšenie transparentnosti používania fondov Spoločenstva. Na druhej strane sa však SDEÚ domnieval, že uverejnenie mien fyzických osôb, ktoré sú príjemcami poľnohospodárskej pomoci z uvedených dvoch fondov, a presných prijatých súm predstavuje neprimerané opatrenie, ktoré so zreteľom na článok 52 ods. 1 Charty nie je oprávnené. Uznané, že v demokratickej spoločnosti je dôležité, aby daňoví poplatníci boli informovaní o využívaní verejných finančných prostriedkov. Keďže „cieľom transparentnosti však nemožno priznať automaticky prednosť pred právom na ochranu osobných údajov“¹⁰³, inštitúcie EÚ boli povinné vyvážiť záujem Únie o transparentnosť s obmedzením uplatňovania práv na súkromie a ochranu údajov, ktoré príjemcovia utrpeli v dôsledku zverejnenia.

SDEÚ dospel k záveru, že inštitúcie EÚ tieto záujmy náležite nevyvážili, keďže do úvahy prichádzali aj opatrenia, ktoré by menej zasahovali do základných práv fyzických osôb a zároveň by účinne prispievali k cieľu zabezpečenia transparentnosti, ktorý sa mal zverejnením dosiahnuť. Napríklad namiesto všeobecného zverejnenia, ktoré sa týka všetkých príjemcov a pri ktorom sa uvádza ich meno a presné sumy, ktoré každý z nich získal, sa mohlo rozlišovať podľa relevantných kritérií, akými sú obdobie poskytovania pomoci, frekvencia poskytovania alebo výška a povaha tejto pomoci¹⁰⁴. SDEÚ tak vyhlásil právne predpisy EÚ o uverejňovaní informácií týkajúcich sa príjemcov pomoci z európskych poľnohospodárskych fondov za čiastočne neplatné.

Príklad: Vo veci *Rechnungshof/Österreichischer Rundfunk a i.*¹⁰⁵ SDEÚ preskúmal zlučiteľnosť niektorých rakúskych právnych predpisov s právnymi predpismi EÚ o ochrane údajov. Právnymi predpismi sa štátnemu orgánu

103 Tamže, bod 85.

104 Tamže, bod 89.

105 SDEÚ, spojené veci C-465/00, C-138/01 a C-139/09, *Rechnungshof/Österreichischer Rundfunk a i., a Christa Neukomm a Joseph Lauermann/Österreichischer Rundfunk*, 20. mája 2003.

ukladala povinnosť zhromažďovať a oznámiť údaje o príjmoch na účely zverejnenia mien a príjmov zamestnancov rôznych verejných subjektov vo výročnej správe, ktorá sa sprístupňuje širokej verejnosti. Niektoré osoby odmietli poskytnúť svoje údaje z dôvodu ochrany údajov.

SDEÚ vo svojom stanovisku vychádzal z toho, že ochrana základných práv je všeobecnou zásadou v rámci práva EÚ, ako aj z článku 8 ECHR, pričom pripomenul, že Charta v tom čase nebola záväzná. Skonštatoval, že získavanie údajov o pracovnom príjme jednotlivca, a najmä ich poskytnutie tretím osobám, patrí do rozsahu pôsobnosti práva na rešpektovanie súkromného života a predstavuje porušenie tohto práva. Tento zásah by mohol byť odôvodnený, ak by bol v súlade s právnymi predpismi, sledoval legitímny cieľ a bol v demokratickej spoločnosti nevyhnutný na dosiahnutie tohto cieľa. SDEÚ uviedol, že rakúska právna úprava sledovala legitímny cieľ, keďže jej cieľom bolo udržať platy verejných zamestnancov v rozumných medziach, pričom ide o dôvod, ktorý súvisí aj s hospodárskou prosperitou krajiny. Záujem Rakúska na zabezpečení čo najlepšieho využitia verejných prostriedkov sa však musel vyvážiť so závažnosťou zásahu do práva dotknutých osôb na rešpektovanie ich súkromného života.

Hoci určiť, či zverejnenie údajov o príjme fyzických osôb bolo nevyhnutné a primerané cieľu, ktorý sa príslušnými právnymi predpismi sleduje, prináleží vnútroštátnemu súdu, SDEÚ tento súd vyzval, aby preskúmal, či tento cieľ nebolo možné dosiahnuť rovnako účinne aj menej rušivým spôsobom. Príkladom by bolo zasielanie osobných údajov len kontrolným verejným orgánom, a nie širokej verejnosti.

Z nasledujúcich prípadov vyplynulo, že vyvažovanie ochrany údajov a prístupu k dokumentom si vyžaduje podrobnú analýzu jednotlivých prípadov. Ani jedno z týchto práv nemôže mať automaticky prednosť pred druhým. SDEÚ mal príležitost na výklad práva na prístup k dokumentom obsahujúcim osobné údaje v dvoch prípadoch.

Príklad: Vo veci *Komisia/Bavarian Lager*¹⁰⁶ SDEÚ vymedzil rozsah ochrany osobných údajov v kontexte prístupu k dokumentom inštitúcií EÚ a vzťah medzi nariadením č. 1049/2001 (nariadenie o prístupe k dokumentom)

106 SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd.* [VK], 29. júna 2010.

a nariadením č. 45/2001 (nariadenie o ochrane údajov inštitúciami EÚ). Spoločnosť Bavarian Lager založená v roku 1992 dováža fľaškové nemecké pivo do Spojeného kráľovstva, najmä pre pohostinstvá a bary. Narazila však na určité ťažkosti, keďže v britských právnych predpisoch sa *de facto* uprednostňovali domáci výrobcovia. Európska komisia v reakcii na sťažnosť spoločnosti Bavarian Lager rozhodla o začatí konania proti Spojenému kráľovstvu z dôvodu neplnenia povinností, ktoré viedlo k zmene sporných ustanovení a ich zosúladieniu s právom EÚ. Spoločnosť Bavarian Lager potom požiadala Komisiu okrem iných dokumentov o kópiu zápisnice zo stretnutia, na ktorom boli prítomní zástupcovia Komisie, britských orgánov a združenia *Confédération des Brasseurs du Marché Commun* (CBMC). Komisia súhlasila so zverejnením určitých dokumentov týkajúcich sa stretnutia, ale vymazala päť mien uvedených v zápisnici, pričom dve osoby výslovne namietali proti zverejneniu svojej totožnosti a zvyšné tri osoby Komisia nebola schopná kontaktovať. Komisia rozhodnutím z 18. marca 2004 zamietla žiadosť spoločnosti Bavarian Lager o poskytnutie úplnej verzie zápisnice zo stretnutia, pričom sa odvolala predovšetkým na ochranu súkromného života týchto osôb zaručenú nariadením o ochrane údajov inštitúciami EÚ.

Spoločnosť Bavarian Lager toto stanovisko neuspokojilo a podala žalobu na Súd prvého stupňa. Tento súd anuloval rozhodnutie Komisie rozsudkom z 8. novembra 2007 (vec T-194/04, *Bavarian Lager/Komisia*), pričom sa opieral o skutočnosť, že uvedenie mien dotknutých osôb v zozname osôb, ktoré sa na stretnutí zúčastnili v mene organizácie, ktorú zastupovali, neznamená zásah do súkromného života a žiadnym spôsobom neohrozuje súkromné životy daných osôb.

Na základe odvolania Komisie SDEÚ anuloval rozsudok Súdu prvého stupňa. SDEÚ dospel k záveru, že v nariadení o prístupe k dokumentom sa stanovuje „špecifický a posilnený režim ochrany osoby, ktorej osobné údaje by prípadne mohli byť oznámené verejnosti“. Podľa SDEÚ platí, že keď je cieľom žiadosti založenej na nariadení o prístupe k dokumentom získanie prístupu k dokumentom obsahujúcim osobné údaje, uplatňujú sa ustanovenia nariadenia o ochrane údajov inštitúciami EÚ v celom ich rozsahu. SDEÚ následne dospel k záveru, že Komisia oprávnené zamietla žiadosť o prístup k celej zápisnici zo stretnutia z októbra 1996. Keďže Komisia nezískala súhlas piatich účastníkov tohto stretnutia, svoju povinnosť otvorenosti dostatočne splnila tým, že zverejnila verziu predmetného dokumentu s vymazanými menami.

Navyše, keďže podľa rozsudku SDEÚ „Bavarian Lager neposkytla žiadne výslovné ani legitímne odôvodnenie, ani žiadny presvedčivý argument s cieľom preukázať potrebu prenosu týchto osobných údajov, Komisia nemohla porovnať rôzne záujmy predmetných subjektov. Nemohla ani preveriť, či nie je nijaký dôvod predpokladať, že týmto prenosom by mohli byť dotknuté legitímne záujmy dotknutých osôb“, ako sa stanovuje v nariadení o ochrane údajov inštitúciami EÚ.

Príklad: Vo veci *ClientEarth a PAN Europe/EFSA*¹⁰⁷ SDEÚ skúmal, či rozhodnutie Európskeho úradu pre bezpečnosť potravín (EFSA) zamietnuť žiadateľom úplný prístup k dokumentom bolo potrebné na ochranu práv na ochranu súkromia a údajov osôb, ktorých sa dokumenty týkajú. Tieto dokumenty sa týkali správy o návrhu usmernení o uvádzaní prípravkov na ochranu rastlín na trh, ktorú vypracovala pracovná skupina EFSA v spolupráci s externými odborníkmi. EFSA pôvodne poskytol žiadateľom čiastočný prístup, pričom im odoprel prístup k niektorým pracovným verziám návrhu usmernení. Následne poskytol prístup k návrhu znenia, ktorý obsahoval individuálne pripomienky externých odborníkov. Odstránil však mená týchto odborníkov, pričom sa odvolal na článok 4 ods. 1 písm. b) nariadenia č. 45/2001 o spracovaní osobných údajov inštitúciami a orgánmi EÚ a na potrebu chrániť súkromie externých odborníkov. Všeobecný súd EÚ v prvom stupni potvrdil rozhodnutie EFSA.

V odvolacom konaní SDEÚ zmenil rozsudok prvostupňového súdu. Dospel k záveru, že prenos osobných údajov v tomto prípade bol potrebný na preverenie nestrannosti každého z externých odborníkov pri plnení vedeckých úloh a na zabezpečenie toho, aby rozhodovací proces v EFSA bol aj naďalej transparentný. SDEÚ konštatoval, že EFSA neuviedol, ako by zverejnením mien externých odborníkov, ktorí predložili konkrétne pripomienky k návrhu usmernení, mohli byť dotknuté oprávnené záujmy týchto odborníkov. Všeobecné tvrdenie, že zverejnenie informácií by mohlo narušiť súkromie, nestačí, ak nie je podložené osobitnými dôkazmi pre každý jednotlivý prípad.

Podľa týchto rozsudkov si zásah do práva na ochranu údajov v súvislosti s prístupom k dokumentom vyžaduje osobitný a oprávnený dôvod. Právo na prístup k dokumentom nemôže automaticky mať prednosť pred právom na ochranu údajov¹⁰⁸.

¹⁰⁷ SDEÚ, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Európsky úrad pre bezpečnosť potravín (EFSA)*, Európska komisia, 16. júla 2015.

¹⁰⁸ Pozri však podrobné rokovania EDPS (2011), Verejný prístup k dokumentom obsahujúcim osobné údaje po vynesení rozsudku Bavarian Lager, Brusel, 24. marca 2011.

Tento **prístup** je podobný prístupu ESĽP, pokiaľ ide o súkromie a prístup k dokumentom, ako to vyplýva aj z nasledujúceho rozsudku. V rozsudku vo veci *Magyar Helsinki* ESĽP konštatoval, že v článku 10 sa jednotlivcovi nepriznáva právo na prístup k informáciám, ktorými disponuje orgán verejnej moci, ani sa štátu neukladá povinnosť jednotlivcovi takéto informácie poskytnúť. Takéto právo alebo povinnosť by však mohli vzniknúť – po prvé, ak sa zverejnenie informácií uloží právoplatným súdnym príkazom; po druhé, ak má prístup k informáciám zásadný význam pre výkon práva jednotlivca na slobodu prejavu – najmä pokiaľ ide o právo prijímať a šíriť informácie – a ak by odmietnutie prístupu predstavovalo zásah do tohto práva¹⁰⁹. Skutočnosť, či a do akej miery odmietnutie prístupu k informáciám predstavuje zásah do slobody prejavu sťažovateľa, sa musí posúdiť vzhľadom na osobitné okolnosti každého jednotlivého prípadu, a to vrátane: i) účelu žiadosti o informácie; ii) povahy požadovaných informácií; iii) úlohy žiadateľa; a iv) či informácie boli pripravené a dostupné.

Príklad: Vo veci *Magyar Helsinki Bizottság/Maďarsko*¹¹⁰ sťažovateľka, ktorou bola mimovládna organizácia pôsobiaca v oblasti ľudských práv, požiadala políciu o informácie týkajúce sa práce obhajcu *ex offio*, aby mohla dokončiť štúdiu o fungovaní systému verejných obhajcov v Maďarsku. Polícia odmietla poskytnúť tieto informácie, pričom tvrdila, že ide o osobné údaje, ktoré nie sú predmetom zverejnenia. ESĽP na základe vyššie uvedených kritérií rozhodol, že došlo k zásahu do práva chráneného podľa článku 10. Presnejšie povedané, sťažovateľka chcela uplatňovať právo šíriť informácie týkajúce sa záležitosti verejného záujmu a požiadala preto o prístup k informáciám na tento účel, pričom tieto informácie boli nevyhnutné na uplatnenie práva sťažovateľky na slobodu prejavu. Informácie o vymenovaní verejných obhajcov boli predmetom verejného záujmu. Niet dôvodu pochybovať o tom, že daná štúdia obsahovala informácie, ktoré sťažovateľka zamýšľala poskytnúť verejnosti a verejnosť mala právo sa ich dozvedieť. ESĽP sa teda domnieval, že prístup k požadovaným informáciám bol nevyhnutný na to, aby sťažovateľka mohla splniť svoju úlohu. Napokon, informácie boli pripravené a dostupné.

ESĽP preto dospel k záveru, že odmietnutie prístupu k informáciám v tomto prípade zasiahlo do samotnej podstaty slobody prijímať informácie. Preskúmal pritom najmä účel požadovaných informácií a ich prínos k dôležitej

109 ESĽP, *Magyar Helsinki Bizottság/Maďarsko* [VK], č. 18030/11, 8. novembra 2016, bod 148.

110 Tamže, body 181, 187 – 200.

verejnej diskusii, povahu požadovaných informácií a skutočnosť, či boli predmetom verejného záujmu, ako aj úlohu, ktorú v danom prípade v spoločnosti zohrávala sťažovateľka.

Vo svojom odôvodnení ESĽP uviedol, že štúdia mimovládnej organizácie sa týkala výkonu spravodlivosti a práva na spravodlivý proces, pričom toto právo má podľa ECHR prvoradý význam. Keďže požadované informácie nezahtíňali údaje mimo verejnej sféry, práva dotknutých osôb (verejní obhajcovia *ex offio*) na súkromie by neboli ohrozené, ak by polícia sťažovateľke prístup k týmto informáciám poskytla. Sťažovateľka požadovala informácie štatistickej povahy, ktoré sa týkali počtu prípadov, v ktorých bol obhajca *ex offio* poverený zastupovaním obžalovaných v trestnom konaní.

ESĽP sa domnieval, že vzhľadom na to, že cieľom štúdie bolo prispieť k dôležitej diskusii o otázkach všeobecného záujmu, by akékoľvek obmedzenia týkajúce sa jej navrhovaného zverejnenia mimovládnu organizáciu mali podliehať obzvlášť dôkladnej kontrole. Predmetné informácie boli predmetom verejného záujmu, keďže verejný záujem sa vzťahuje na „záležitosti, ktoré môžu vyvolať značnú polemiku, ktoré sa týkajú dôležitej spoločenskej otázky, alebo ktoré sa týkajú problému, o ktorom by verejnosť mala záujem byť informovaná“¹¹¹. Nepochybne by tu patrila aj diskusia o výkone spravodlivosti a spravodlivosti súdnych procesov, ktorá bola predmetom štúdie sťažovateľky. Po vyvážení jednotlivých dotknutých práv a uplatnení zásady proporcionality ESĽP dospel k záveru, že došlo k neodôvodnenému porušeniu práv sťažovateľky podľa článku 10 ECHR.

1.3.2. Služobné tajomstvo

Podľa vnútroštátneho práva môže určitá komunikácia podliehať povinnosti služobného tajomstva. Služobné tajomstvo sa chápe ako osobitná etická povinnosť, pri ktorej vzniká zákonná povinnosť súvisiaca s určitými povolaniami a funkciami, ktoré sú založené na viere a dôvere. Osoby a inštitúcie, ktoré vykonávajú tieto funkcie, nesmú zverejňovať dôverné informácie, ktoré získali pri plnení svojich povinností. Služobné tajomstvo sa týka najmä lekárskej profesie a povinnosti advokáta zachovávať mlčanlivosť, pričom v mnohých jurisdikciách sa uznáva aj povinnosť služobného tajomstva vo finančnom sektore. Služobné tajomstvo nie je základným

¹¹¹ Tamže, bod 156.

právom, ale je chránené ako forma práva na rešpektovanie súkromného života. SDEÚ napríklad rozhodol, že v určitých prípadoch „môže byť potrebné zakázať sprístupnenie určitých informácií považovaných za dôverné, aby sa zachovalo základné právo podniku na dodržiavanie súkromného života, zakotvené v článku 8 ECHR [...] a v článku 7 Charty“.¹¹² ESLP už tiež rozhodoval o tom, či sú obmedzenia týkajúce sa služobného tajomstva porušením článku 8 ECHR, ako sa uvádza vo zvýraznených príkladoch.

Príklad: Vo veci *Pruteanu/Rumunsko*¹¹³ sťažovateľ vystupoval ako advokát obchodnej spoločnosti, ktorej bolo na základe obvinení z podvodu zakázané uskutočňovanie bankových transakcií. Počas vyšetrovania prípadu rumunské súdy povolili orgánom činným v trestnom konaní počas určitého obdobia odpočúvať a zaznamenávať telefonické rozhovory spoločníka spoločnosti. Záznamy a odpočúvanie zahŕňali jeho komunikáciu s advokátom.

Pán Pruteanu tvrdil, že išlo o zásah do jeho práva na rešpektovanie súkromného života a korešpondencie. ESLP vo svojom rozsudku zdôraznil postavenie a význam vzťahu advokáta s jeho klientom. Pri odpočúvaní telefonických rozhovorov s jeho klientom nepochybne išlo o porušovanie služobného tajomstva, ktoré bolo základom vzťahu medzi týmito dvoma osobami. V takom prípade by sa advokát mohol sťažovať aj na zásah do jeho práva na rešpektovanie súkromného života a korešpondencie. SDEÚ dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Príklad: Vo veci *Brito Ferrinho Bexiga Villa-Nova/Portugalsko*¹¹⁴ sťažovateľka, pôsobiaca ako advokátka, odmietla sprístupniť svoje osobné bankové výpisy daňovým úradom z dôvodu služobného tajomstva a bankového tajomstva. Prokuratúra začala vyšetrovanie vo veci daňového podvodu a požiadala o zrušenie uplatňovania služobného tajomstva. Vnútroštátne súdy nariadili zrušenie uplatňovania služobného a bankového tajomstva, pričom konštatovali, že verejný záujem by mal mať prednosť pred súkromnými záujmami sťažovateľky.

112 SDEÚ, vec T-462/12 R, *Pilkington Group Ltd/Európska komisia*, uznesenie predsedu Všeobecného súdu, 11. marca 2013, bod 44.

113 ESLP, *Pruteanu/Rumunsko*, č. 30181/05, 3. februára 2015.

114 ESLP, *Brito Ferrinho Bexiga Villa-Nova/Portugalsko*, č. 69436/10, 1. decembra 2015.

Po predložení veci ESĽP tento súd konštatoval, že prístup k bankovým výpisom sťažovateľky predstavuje zásah do jej práva na rešpektovanie služobného tajomstva, ktoré je súčasťou súkromného života. Tento zásah mal právny základ, keďže vychádzal z trestného poriadku, a sledoval legitímny cieľ. Pri skúmaní nevyhnutnosti a primeranosti zásahu však ESĽP poukázal na skutočnosť, že konanie o zrušení dôvernosti sa uskutočnilo bez účasti alebo vedomia sťažovateľky. Sťažovateľka sa teda nemohla k nemu vyjadriť. Okrem toho, hoci sa vo vnútroštátnom práve stanovovalo, že pri takomto konaní je potrebné konzultovať so združením advokátov, k tejto konzultácii nedošlo. Sťažovateľka navyše nemala možnosť účinne spochybniť zrušenie dôvernosti ani využiť opravný prostriedok na napadnutie tohto opatrenia. Vzhľadom na nedostatok procesných záruk a účinnej súdnej kontroly vo vzťahu k opatreniu, ktorým sa pozastavuje povinnosť zachovávať dôvernosť, ESĽP dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Vzájomné pôsobenie medzi služobným tajomstvom a ochranou údajov je často nejednoznačné. Na jednej strane pravidlá ochrany údajov a záruky stanovené v právnych predpisoch pomáhajú zabezpečovať zachovávanie služobného tajomstva. Napríklad cieľom pravidiel, ktorými sa od prevádzkovateľov a sprostredkovateľov vyžaduje, aby prijímali spoľahlivé opatrenia v oblasti bezpečnosti údajov, je okrem iného zabrániť strate dôvernosti osobných údajov chránených služobným tajomstvom. Okrem toho sa vo všeobecnom nariadení EÚ o ochrane údajov umožňuje spracúvanie údajov týkajúcich sa zdravia, ktoré predstavujú osobitné kategórie osobných údajov, ktoré si vyžadujú silnejšiu ochranu, toto spracúvanie sa však podmieňuje prijatím vhodných a osobitných opatrení na ochranu práv dotknutých osôb, najmä pokiaľ ide o služobné tajomstvo¹¹⁵.

Na druhej strane povinnosti služobného tajomstva uložené prevádzkovateľom a sprostredkovateľom v súvislosti s určitými osobnými údajmi môžu obmedziť práva dotknutých osôb, najmä právo na prijímanie informácií. Hoci všeobecné nariadenie o ochrane údajov obsahuje rozsiahly zoznam informácií, ktoré sa v zásade musia poskytnúť dotknutej osobe v prípade, že osobné údaje neboli získané od nej, táto požiadavka sa neuplatňuje v prípade, ak osobné údaje musia zostať dôverné na základe povinnosti zachovania služobného tajomstva upravenej právom Únie alebo právom členského štátu¹¹⁶.

115 Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. h) a článok 9 ods. 3.

116 Tamže, článok 14 ods. 5 písm. d).

Všeobecné nariadenie o ochrane údajov (GDPR) umožňuje, aby členské štáty v právnych predpisoch prijali osobitné pravidlá s cieľom zaručiť plnenie povinností týkajúcich sa služobného tajomstva alebo inej rovnocennej povinnosti zachovávať mlčanlivosť a zosúladiť právo na ochranu osobných údajov s povinnosťou služobného tajomstva¹¹⁷.

V GDPR sa stanovuje, že členské štáty môžu prijať osobitné pravidlá týkajúce sa právomocí dozorných orgánov vo vzťahu k prevádzkovateľom alebo sprostredkovateľom, na ktorých sa vzťahuje povinnosť služobného tajomstva. Tieto osobitné pravidlá sa týkajú právomoci získať prístup do priestorov prevádzkovateľa alebo sprostredkovateľa, k jeho zariadeniam na spracúvanie údajov a uchovávaným osobným údajom, ak takéto osobné údaje boli získané v rámci činnosti, na ktorú sa vzťahuje povinnosť zachovávať mlčanlivosť. Dozorné orgány poverené ochranou údajov musia preto rešpektovať povinnosti služobného tajomstva, ktorým podliehajú prevádzkovatelia a sprostredkovatelia. Okrem toho podliehajú povinnosti zachovávať služobné tajomstvo aj členovia dozorných orgánov, a to počas a po skončení ich funkčného obdobia. Členovia a zamestnanci dozorných orgánov môžu pri plnení svojich úloh získať dôverné informácie. V článku 54 ods. 2 nariadenia sa jasne stanovuje povinnosť zachovávať služobné tajomstvo, pokiaľ ide o dôverné informácie.

Podľa GDPR sa vyžaduje, aby členské štáty oznámili Komisii pravidlá, ktoré prijímú na zosúladenie ochrany údajov a zásad stanovených v nariadení s povinnosťou zachovávať služobné tajomstvo.

1.3.3. Sloboda náboženského vyznania a viery

Sloboda náboženského vyznania a viery je chránená článkom 9 ECHR (sloboda myslenia, svedomia a náboženského vyznania) a článkom 10 Charty základných práv EÚ. Osobné údaje, ktoré odhaľujú náboženské alebo filozofické presvedčenie, sa v právnych predpisoch EÚ, ako aj v právnych predpisoch RE považujú za „citlivé údaje“ a ich spracúvanie a používanie podlieha zvýšenej ochrane.

Príklad: Sťažovateľ vo veci *Sinan Işık/Turecko*¹¹⁸ bol príslušníkom náboženskej komunity Alevitov, ktorej viera je ovplyvnená sufizmom a inými predislamskými presvedčeniami, a niektorí vedci ho považujú za samostatné náboženstvo a iní za súčasť islamského náboženstva. Sťažovateľ namietal, že jeho preukaz totožnosti v rozpore s jeho želaniami obsahuje rubriku, v ktorej sa

¹¹⁷ Tamže, odôvodnenie 164 a článok 90.

¹¹⁸ ESLP, *Sinan Işık/Turecko*, č. 21924/05, 2. februára 2010.

jeho náboženstvo označuje ako „islam“, a nie ako „alevitské“. Vnútroštátne súdy zamietli jeho žiadosť o zmenu v preukaze totožnosti na „alevitské“ z dôvodu, že tento pojem označuje podskupinu islamu, a nie samostatné náboženstvo. Následne sa na ESLP sťažoval, že bol nútený zverejniť svoju vieru bez udelenia súhlasu, pretože na preukaze totožnosti bolo povinné označiť náboženstvo osoby, a že to bolo v rozpore s jeho právom na slobodu náboženského vyznania a svedomím, najmä vzhľadom na to, že označenie „islam“ na jeho preukaze totožnosti bolo nesprávne.

ESLP zdôraznil, že náboženská sloboda zahŕňa slobodu prejavovať svoje náboženské vyznanie v rámci komunity, na verejnosti a v rámci okruhu osôb, ktoré majú rovnakú vieru, ale aj samostatne a v súkromí. Z vnútroštátnych právnych predpisov platných v tom čase vyplývala povinnosť jednotlivcov nosiť preukaz totožnosti, dokument, ktorým sa museli preukázať na žiadosť ktoréhokoľvek orgánu verejnej moci alebo súkromného podniku a na ktorom sa uvádzalo ich náboženské vyznanie. Pri takejto povinnosti sa nezohľadňovala skutočnosť, že právo prejavovať náboženské vyznanie predstavuje aj opak, t. j. právo nebyť povinný zverejniť svoje presvedčenie. Hoci vláda tvrdila, že vnútroštátne právne predpisy boli zmenené tak, aby jednotlivci mohli požiadať, aby rubrika náboženstvo v ich preukaze totožnosti zostala prázdna, podľa názoru súdu by samotná potreba požiadať o vymazanie údajov o náboženstve mohla predstavovať zverejnenie informácie o postoji k náboženstvu. Okrem toho, ak majú preukazy totožnosti rubriku na údaj o náboženstve, má určitý význam aj to, ak je ponechaná prázdna, keďže držiteľia preukazu totožnosti bez údajov o náboženstve by sa líšili od tých, ktorí v preukaze náboženstvo uvedené majú. ESLP dospel k záveru, že vnútroštátne právne predpisy boli v rozpore s článkom 9 ECHR.

Činnosť cirkví a náboženských združení alebo spoločností si môže vyžadovať spracúvanie osobných údajov členov, aby sa umožnila komunikácia a organizácia činností v rámci kongregácie. Cirkvi a náboženské združenia teda často zavádzajú pravidlá týkajúce sa spracúvania osobných údajov. Podľa článku 91 všeobecného nariadenia o ochrane údajov, ak sú tieto pravidlá komplexné, môžu sa naďalej uplatňovať za predpokladu, že sú zosúladené s ustanoveniami nariadenia. Cirkvi a náboženské združenia, ktoré uplatňujú takéto pravidlá, podliehajú dohľadu zo strany nezávislého dozorného orgánu, ktorý môže mať osobitnú povahu, pokiaľ spĺňajú podmienky stanovené vo všeobecnom nariadení o ochrane údajov¹¹⁹.

119 Všeobecné nariadenie o ochrane údajov, článok 91 ods. 2.

Náboženské organizácie môžu vykonávať spracúvanie osobných údajov z viacerých dôvodov – napríklad na udržiavanie kontaktu so svojou kongregáciou alebo na sprostredkovanie informácií o náboženských alebo charitatívnych podujatiach a iných podujatiach, ktoré sa organizujú. V niektorých štátoch cirkvi musia viesť evidenciu svojich členov z daňových dôvodov, pretože členstvo v náboženských organizáciách môže mať vplyv na daňovú povinnosť jednotlivcov. V každom prípade, podľa európskeho práva sú údaje odhaľujúce náboženské presvedčenie citlivými údajmi a cirkvi musia niesť zodpovednosť za zaobchádzanie s takýmito údajmi a ich spracúvanie, najmä preto, že informácie spracúvané náboženskými organizáciami sa často týkajú detí, starších ľudí alebo iných zraniteľných členov spoločnosti.

1.3.4. Sloboda umenia a vedeckého bádania

Ďalším právom, ktoré je potrebné vyvažovať voči právom na rešpektovanie súkromného života a ochranu údajov, je sloboda umenia a vedeckého bádania, ktorá je výslovne chránená podľa článku 13 Charty základných práv Európskej únie. Toto právo sa primárne odvodzuje od práva na slobodu myslenia a prejavu a má sa vykonávať so zreteľom na článok 1 Charty (ľudská dôstojnosť). ESĽP sa domnieva, že sloboda umenia je chránená na základe článku 10 ECHR¹²⁰. Na právo zaručené článkom 13 Charty sa môžu vzťahovať obmedzenia vyplývajúce z článku 52 ods. 1 Charty, ktoré je možné vykladať aj podľa článku 10 ods. 2 ECHR¹²¹.

Príklad: Vo veci *Vereinigung bildender Künstler/Rakúsko*¹²² rakúske súdy zakázali združeniu sťažovateľa, aby vystavovalo obraz, ktorý obsahoval fotografie hláv rôznych verejne známych osobností v sexuálnych polohách. Poslanec rakúskeho parlamentu, ktorého fotografia bola na obraze použitá, zažaloval združenie sťažovateľa a žiadal vydanie súdneho príkazu, ktorý by zakázal vystavovanie predmetného obrazu. Vnútroštátny súd vydal takýto súdny príkaz. ESĽP pripomenul, že článok 10 ECHR sa uplatňuje aj na šírenie myšlienok, ktoré urážajú, poburujú alebo znepokojujú štát či niektorú časť obyvateľstva. Osoby, ktoré vytvorili, predviedli, šíрили alebo vystavili umelecké dielo, sa podieľali na šírení myšlienok a stanovísk a štát má povinnosť nezasahovať neprimerane proti ich slobode prejavu. Vzhľadom na to, že obraz predstavoval koláž, v ktorej boli použité iba hlavy osôb a ich telá boli namaľované nereálne a zveličené tak, že obraz zjavne nemal odrážať či dokonca

120 ESĽP, *Müller a i./Švajčiarsko*, č. 10737/84, 24. mája 1988.

121 Vysvetlivky k Charte základných práv, Ú. v. ES C 303, 2007.

122 ESĽP, *Vereinigung bildender Künstler/Rakúsko*, č. 68354/01, 25. januára 2007, body 26 a 34.

naznačovať realitu, EŠLP ďalej uviedol, že „obraz ťažko možno chápať tak, že by opisoval podrobnosti súkromného života [znázornenej osoby], ale týka sa skôr jej verejného postavenia politika“ a že „[znázornená osoba] musí vo svojej funkcii prejavovať väčšiu toleranciu voči kritike“. EŠLP zvážil rôzne dotknuté záujmy a konštatoval, že neobmedzený zákaz ďalšieho vystavovania obrazu bol neprimeraný. Súd dospel k záveru, že došlo k porušeniu článku 10 ECHR.

V európskych právnych predpisoch o ochrane údajov sa zohľadňuje aj osobitná hodnota vedeckého bádania pre spoločnosť. Všeobecné nariadenie o ochrane údajov a modernizovaný Dohovor č. 108 umožňujú uchovávanie údajov na dlhšie obdobia, pokiaľ sa osobné údaje spracúvajú výlučne na účely vedeckého alebo historického výskumu. Okrem toho a bez ohľadu na pôvodný účel konkrétnej spracovateľskej činnosti sa následné využívanie osobných údajov na vedecký výskum nepovažuje za nezlučiteľný účel¹²³. Zároveň sa pri takomto spracúvaní musia zaviesť primerané záruky na ochranu práv a slobôd dotknutých osôb. V právnych predpisoch EÚ alebo členských štátov sa môžu stanoviť odchýlky od práv dotknutej osoby, ako je napríklad právo na prístup, opravu, obmedzenie spracúvania a právo namietat', pokiaľ ide o spracúvanie jej osobných údajov na účely vedeckého výskumu, na historické alebo štatistické účely (pozri aj [oddiel 6.1](#) a [oddiel 9.4](#)).

1.3.5. Ochrana duševného vlastníctva

Právo na ochranu majetku je zakotvené v článku 1 dodatkového protokolu k ECHR, ako aj v článku 17 ods. 1 Charty základných práv EÚ. Jedným z dôležitých aspektov práva vlastníť majetok, ktorý je obzvlášť relevantný z hľadiska ochrany údajov, je ochrana duševného vlastníctva, výslovne uvedená v článku 17 ods. 2 Charty. Viacere smernice v rámci právneho poriadku EÚ majú za cieľ účinne chrániť duševné vlastníctvo, najmä autorské práva. Duševné vlastníctvo zahŕňa nielen literárne a umelecké vlastníctvo, ale aj patenty, ochranné známky a súvisiace práva.

Z judikatúry SDEÚ vyplýva, že ochrana základného práva vlastníť majetok musí byť vyvážená s ochranou ostatných základných práv, najmä práva na ochranu údajov¹²⁴. Vyskytli sa prípady, keď inštitúcie na ochranu autorských práv žiadali, aby

¹²³ Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. b) a modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b).

¹²⁴ SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [VK], 29. januára 2008, body 62 – 68.

poskytovatelia internetového pripojenia zverejnili totožnosť používateľov platforiem na výmenu súborov na internete. Takéto platformy často umožňujú používateľom internetu sťahovať si hudobné tituly bezplatne, hoci sú chránené autorským právom.

Príklad: *Vec Promusicae/Telefónica de España*¹²⁵ sa týka odmietnutia španielskeho poskytovateľa internetového pripojenia – spoločnosti Telefónica – vyhovieť požiadavke neziskovej organizácie hudobných producentov a vydavateľov hudobných a audiovizuálnych záznamov Promusicae, aby spoločnosť Telefónica zverejnila osobné údaje určitých osôb, ktorým poskytuje služby internetového pripojenia. Spoločnosť Promusicae požadovala zverejnenie informácií, aby mohla začať občianske súdne konanie proti tým osobám, o ktorých tvrdila, že používali program na vzájomnú výmenu súborov umožňujúci prístup ku zvukovým záznamom, pričom práva na využívanie týchto súborov majú členovia organizácie Promusicae.

Španielsky súd postúpil vec SDEÚ a položil otázku, či takéto osobné údaje musia byť podľa práva Spoločenstva oznámené v kontexte občianskoprávneho konania s cieľom zaistiť efektívnu ochranu autorských práv. Odkázal pritom na smernice 2000/31, 2001/29 a 2004/48 v zmysle článkov 17 a 47 Charty. SDEÚ dospel k názoru, že v týchto troch smerniciach, ako aj v smernici o súkromí a elektronických komunikáciách (smernica 2002/58) sa členským štátom nebráni, aby stanovili povinnosť zverejňovať osobné údaje v súvislosti s občianskoprávnymi konaniami s cieľom zaistiť efektívnu ochranu autorských práv.

SDEÚ poukázal na to, že v tejto veci vyplynula otázka potreby zosúladiť požiadavky ochrany rôznych základných práv, predovšetkým práva na rešpektovanie súkromného života, s právami na ochranu vlastníctva a účinného prostriedku nápravy.

Súd dospel k tomuto záveru: „pritom musia členské štáty pri preberaní vyššie uvedených smerníc dbať na to, aby vychádzali z výkladu týchto smerníc, ktorý umožňuje zabezpečiť náležitú rovnováhu medzi rôznymi základnými právami chránenými právnym poriadkom Spoločenstva. Ďalej je potrebné, aby orgány a sudy členských štátov pri vykonávaní opatrení na prebratie týchto smerníc nielen vykladali svoje vnútroštátne právo v súlade s uvedenými smernicami,

125 Tamže, body 54 a 60.

ale takisto dbali na to, aby nevychádzali z výkladu týchto smerníc, ktorý by kolidoval s uvedenými základnými právami alebo s inými všeobecnými zásadami práva Spoločenstva, ako je zásada proporcionality¹²⁶.

Príklad: *Vec Bonnier Audio AB a i./Perfect Communication Sweden AB*¹²⁷ sa týkala hľadania rovnováhy medzi právami duševného vlastníctva a ochranou osobných údajov. Žalobcovia – päť vydavateľstiev s autorskými právami k 27 audioknihám – podali na švédsky súd žalobu, v ktorej tvrdili, že tieto autorské práva boli porušené prostredníctvom servera FTP (protokol prenosu súborov, ktorý umožňuje sprístupňovanie súborov a prenos údajov po internete). Žalobcovia žiadali od poskytovateľa internetových služieb, aby im oznámil meno a adresu osoby používajúcej adresu IP, z ktorej boli súbory zaslané. Poskytovateľ internetových služieb ePhone proti tejto žiadosti namietal, pričom tvrdil, že ide o porušenie smernice 2006/24 (smernice o uchovávaní údajov, ktorá bola zrušená v roku 2014).

Švédsky súd postúpil vec SDEÚ a položil mu otázku, či smernica 2006/24 bráni uplatneniu vnútroštátneho ustanovenia založeného na článku 8 smernice 2004/48 (smernica o vymožitelnosti práv duševného vlastníctva), ktorým sa umožňuje vydať súdny príkaz, ktorým sa poskytovateľom internetových služieb ukladá povinnosť oznámiť držiteľom autorských práv informácie o účastníkoch, ktorých adresy IP boli údajne použité pri porušení práva. Otázka sa zakladá na predpoklade, že žalobca predložil jednoznačné dôkazy o porušení autorského práva a že požadované opatrenie je primerané.

SDEÚ zdôraznil, že smernica 2006/24 sa týka výlučne spracúvania a uchovávania údajov vytvorených poskytovateľmi elektronických komunikačných služieb na účely vyšetrovania, odhaľovania a stíhania závažných trestných činov, ako aj poskytovania týchto údajov príslušným vnútroštátnym orgánom. Vnútroštátne ustanovenie, ktorým sa transponuje smernica o vymožitelnosti práv duševného vlastníctva, teda nepatrí do pôsobnosti smernice 2006/24, a preto mu táto smernica nebráni¹²⁸.

126 Tamže, body 65 a 68; pozri tiež SDEÚ, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16. februára 2012.

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

128 Tamže, body 40 – 41.

Pokiaľ ide o oznámenie mena a adresy, ktorého sa domáhali žalobcovia, SDEÚ rozhodol, že takéto konanie predstavuje spracúvanie osobných údajov a patrí do pôsobnosti smernice 2002/58 (smernica o súkromí a elektronických komunikáciách). Ďalej uviedol, že oznámenie týchto údajov sa požaduje v rámci občianskoprávneho konania v prospech držiteľa autorského práva na zabezpečenie účinnej ochrany autorských práv, a preto patrí vzhľadom na jeho predmet do pôsobnosti smernice 2004/48¹²⁹.

SDEÚ dospel k záveru, že smernice 2002/58 a 2004/48 sa majú vykladať v tom zmysle, že nebránia vnútroštátnej právnej úprave, akou je právna úprava vo veci samej, ktorá vnútroštátnemu súdu, ktorému bol predložený návrh na vydanie príkazu poskytnúť osobné údaje, umožňuje, aby v závislosti od okolností každého jednotlivého prípadu a s náležitým prihliadnutím na požiadavky vyplývajúce zo zásady proporcionality zvážil jednotlivé protichodné záujmy.

1.3.6. Ochrana údajov a hospodárske záujmy

V digitálnom veku alebo veku veľkých dát sa o údajoch často hovorí ako o „novej ropе“ hospodárstva, ktorá podporuje inováciu a tvorivosť¹³⁰. Mnohé spoločnosti si vybudovali stabilné obchodné modely založené na spracúvaní údajov a takéto spracúvanie často zahŕňa osobné údaje. Niektoré spoločnosti sa môžu domnievať, že osobitné pravidlá týkajúce sa ochrany osobných údajov by v praxi viedli k povinnostiam, ktoré sú príliš veľkou záťažou, ktorá by ovplyvnila ich hospodárske záujmy. Objavuje sa teda otázka, či hospodárske záujmy prevádzkovateľov a sprostredkovateľov alebo širokej verejnosti môžu byť dôvodom na obmedzenie práva na ochranu údajov.

Príklad: V rozsudku vo veci *Google Spain*¹³¹ SDEÚ rozhodol, že jednotlivci majú za určitých podmienok právo požadovať od vyhľadávačov, aby vymazali výsledky vyhľadávania zo svojich indexov. SDEÚ vo svojom odôvodnení poukázal na skutočnosť, že na základe používania vyhľadávačov a výsledkov

129 Tamže, body 52 – 54. Pozri aj SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [VK], 29. januára 2008, bod 58.

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

131 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014.

vyhľadávania je možné vytvoriť podrobný profil určitej osoby. Tieto informácie sa môžu týkať mnohých aspektov súkromného života danej osoby a bez vyhľadávača by nebolo možné ich tak ľahko nájsť alebo dať do súvislosti. Išlo teda o potenciálne závažný zásah do základných práv dotknutých osôb na súkromie a ochranu osobných údajov.

SDEÚ následne preskúmal, či by zásah mohol byť odôvodnený. Pokiaľ ide o hospodársky záujem spoločnosti na vykonaní spracúvania, SDEÚ uviedol, že „je nutné konštatovať, že [zásah] nemožno odôvodniť výlučne hospodárskym záujmom poskytovateľa tohto vyhľadávača na tomto spracovaní“ a že „v zásade“ základné práva podľa článkov 7 a 8 Charty prevažujú nad takýmto hospodárskym záujmom a nad záujmom verejnosti nájsť uvedenú informáciu v rámci vyhľadávania na základe mena dotknutej osoby¹³².

Jedným zo základov európskych právnych predpisov o ochrane údajov je poskytnúť jednotlivcom väčšiu kontrolu nad ich osobnými údajmi. Najmä v súčasnom digitálnom veku existuje nerovnováha medzi právomocami obchodných subjektov, ktoré spracúvajú veľké množstvo osobných údajov a majú k takýmto údajom prístup, a právomocami osôb, ktorým tieto osobné údaje patria, pokiaľ ide o kontrolu nad ich informáciami. SDEÚ pri vyvažovaní ochrany údajov a hospodárskych záujmov, ako sú záujmy tretích strán vo vzťahu k akciovým spoločnostiam a spoločnostiam s ručením obmedzeným, posudzuje každý prípad jednotlivo, ako to vyplýva aj z rozsudku vo veci *Manni*.

Príklad: Vec *Manni*¹³³ sa týkala zahrnutia osobných údajov jednotlivca do verejného obchodného registra. Pán Manni požiadal obchodnú komoru v Lecce, aby vymazala jeho osobné údaje z tohto registra po tom, ako zistil, že potenciálni klienti v registri dokázali zistiť, že bol správcom spoločnosti, na ktorú bol pred viac ako desiatimi rokmi vyhlásený konkurz. Tieto informácie vzbudzovali u jeho potenciálnych klientov negatívny dojem a mohli by mať negatívny vplyv na jeho obchodné záujmy.

132 Tamže, body 81 a 97.

133 SDEÚ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9. marca 2017.

SDEÚ bol požiadaný, aby určil, či sa v tomto prípade uplatňuje právo na výmaz podľa právnych predpisov EÚ. SDEÚ sa vo svojom závere usiloval o vyváženie pravidiel ochrany údajov EÚ a obchodného záujmu pána Manniho na odstránení informácií o konkurze jeho bývalej spoločnosti s verejným záujmom na prístupe k informáciám. Vzal na vedomie skutočnosť, že zverejnenie informácií vo verejnom registri spoločností vyplývalo zo zákona a najmä zo smernice EÚ, ktorej cieľom je uľahčiť prístup tretích strán k informáciám o spoločnostiach. Zverejnenie bolo dôležité z dôvodu ochrany záujmov tretích strán, ktoré môžu mať záujem o obchodovanie s konkrétnou spoločnosťou, pretože akciové spoločnosti a spoločnosti s ručením obmedzeným ručia vo vzťahu k tretím osobám iba svojím majetkom. Na tento účel „má zverejnenie tretím osobám umožniť oboznámiť sa s podstatnými dokladmi spoločnosti, ako aj s niektorými údajmi o nej, najmä údajmi o osobách, ktoré sú oprávnené zaväzovať spoločnosť“¹³⁴.

Vzhľadom na dôležitosť legitímneho cieľa sledovaného registrom SDEÚ konštatoval, že pán Manni nemá právo požadovať vymazanie svojich osobných údajov, keďže potreba chrániť záujmy tretích osôb vo vzťahu k akciovým spoločnostiam a spoločnostiam s ručením obmedzeným a zabezpečiť právnu istotu, ako aj poctivosť v obchodnom styku, a teda riadne fungovanie vnútorného trhu, majú prednosť pred jeho právami podľa právnych predpisov o ochrane údajov. Platí to najmä vzhľadom na skutočnosť, že osoby, ktoré sa rozhodnú podieľať na hospodárskom živote formou akciovej spoločnosti alebo spoločnosti s ručením obmedzeným, sú si vedomé povinnosti zverejniť údaje o svojej totožnosti a funkciách.

Hoci SDEÚ konštatoval, že v tomto prípade neexistujú dôvody na dosiahnutie výmazu údajov, uznal existenciu práva namietat' proti spracúvaniu, pričom uviedol: „nemožno vylúčiť, že existujú osobitné situácie, v ktorých je z prevažujúcich a legitímnych dôvodov vyplývajúcich z konkrétneho prípadu dotknutej osoby a po uplynutí dostatočne dlhej lehoty [...] výnimočne odôvodnené obmedziť prístup k jej osobným údajom zapísaným v registri na tretie osoby, ktoré preukážu osobitný záujem na nahliadnutí do týchto údajov“¹³⁵.

134 Tamže, bod 49.

135 Tamže, bod 60.

SDEÚ uviedol, že vnútroštátnym súdom prináleží, aby v každom jednotlivom prípade a so zreteľom na všetky relevantné okolnosti konkrétnej osoby posúdili existenciu alebo neexistenciu oprávnených a prevažujúcich dôvodov, ktoré by mohli výnimočne odôvodniť obmedzenie prístupu tretích strán k osobným údajom obsiahnutým v registroch spoločností. Objasnil však, že pokiaľ ide o pána Manniho, samotná skutočnosť, že zverejnenie jeho osobných údajov v registri údajne ovplyvnilo jeho zákazníkov, sa nemôže považovať za oprávnený a prevažujúci dôvod. Potenciálni klienti pána Manniho majú oprávnený záujem získať informácie týkajúce sa konkurzu jeho predchádzajúcej spoločnosti.

V prípade pána Manniho a iných osôb uvedených v registri zásah do základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, ako sú zaručené v článku 7 a 8 Charty, slúžil cieľu všeobecného záujmu a bol nevyhnutný a primeraný.

Vo veci *Manni* preto SDEÚ rozhodol, že práva na ochranu údajov a súkromia neprevážujú nad záujmom tretích strán na prístupe k informáciám v registri spoločností vo vzťahu k akciovým spoločnostiam a spoločnostiam s ručením obmedzeným.

2

Terminológia v oblasti ochrany údajov

EÚ	Zahrnuté témy	RE
Osobné údaje		
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 1	Právne vymedzenie ochrany údajov	Modernizovaný Dohovor č. 108, článok 2 písm. a)
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 5 a článok 5 ods. 1 písm. e)		ESLP, <i>Bernh Larsen Holding AS a i./Nórsko</i> , č. 24117/08, 2013
Všeobecné nariadenie o ochrane údajov, článok 9		ESLP, <i>Uzun/Nemecko</i> , č. 35623/05, 2010
SDEÚ, spojené veci C-92/09 a C-93/09, <i>Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen</i> [VK], 2010		ESLP, <i>Amann/Švajčiarsko</i> [VK], č. 27798/95, 2000
SDEÚ, C-275/06, <i>Productores de Música de España (Promusicae)/Telefónica de España SAU</i> [VK], 2008		
SDEÚ, C-70/10, <i>Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)</i> , 2011		
SDEÚ, C-582/14, <i>Patrick Breyer/Bundesrepublik Deutschland</i> , 2016		
SDEÚ, spojené veci C-141/12 a C-372/12, <i>YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S</i> , 2014	Osobitné kategórie osobných údajov (citlivé údaje)	
SDEÚ, C-101/01, <i>Trestné konanie proti Bodil Lindqvist</i> , 2003		Modernizovaný Dohovor č. 108, článok 6 ods. 1

EÚ	Zahrnuté témy	RE
SDEÚ, C-434/16, <i>Peter Nowak/Data Protection Commissioner</i> , 2017	Anonymizované a pseudonymizované osobné údaje	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. e) Dôvodová správa k modernizovanému Dohovoru č. 108, odsek 50.
Spracúvanie údajov		
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 2 SDEÚ, C-212/13, <i>František Ryneš/Úřad pro ochranu osobních údajů</i> , 2014 SDEÚ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni</i> , 2017 SDEÚ, C-101/01, <i>Trestné konanie proti Bodil Lindqvist</i> , 2003 SDEÚ, C-131/12, <i>Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD)</i> , Mario Costeja González [VK], 2014	Vymedzenia pojmov	Modernizovaný Dohovor č. 108, článok 2 písm. b) a c)
Používatelia údajov		
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 7 SDEÚ, C-212/13, <i>František Ryneš/Úřad pro ochranu osobních údajů</i> , 2014 SDEÚ, C-1318/12, <i>Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD)</i> , Mario Costeja González [VK], 2014	Prevádzkovateľ	Modernizovaný Dohovor č. 108, článok 2 písm. d) Odporúčanie o profilovaní, článok 1 písm. g)*
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 8	Sprostredkovateľ	Modernizovaný Dohovor č. 108, článok 2 písm. f) Odporúčanie o profilovaní, článok 1 písm. h)
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 9	Príjemca	Modernizovaný Dohovor č. 108, článok 2 písm. e)
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 10	Tretia strana	

EÚ	Zahrnuté témy	RE
Súhlas		
Všeobecné nariadenie o ochrane údajov, článok 4 ods. 11 a článok 7 SDEÚ, C-543/09, <i>Deutsche Telekom AG/Bundesrepublik Deutschland</i> , 2011 SDEÚ, C-536/15, <i>Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)</i> , 2017	Vymedzenie platného súhlasu a požiadavky naň	Modernizovaný Dohovor č. 108, článok 5 ods. 2 Odporúčanie o zdravotných údajoch, článok 6 a ďalšie následné odporúčania ESLP, <i>Elberte/Lotyško</i> , č. 61243/08, 2015

Poznámka: *Rada Európy, Výbor ministrov (2010), Odporúčanie Rec(2010)13 členským štátom o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania (odporúčanie o profilovaní), 23. novembra 2010.

2.1. Osobné údaje

Hlavné body

- Údaje sú osobnými údajmi vtedy, keď sa týkajú identifikovanej alebo aspoň identifikovateľnej osoby, „dotknutá osoba“.
- Pri určovaní toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, napríklad osobitný výber, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, na priamu alebo nepriamu identifikáciu fyzickej osoby.
- Autentifikácia znamená poskytnutie dôkazu o tom, že určitá osoba má určitú totožnosť a/alebo je oprávnená vykonávať určité činnosti.
- Existujú osobitné kategórie údajov, tzv. citlivé údaje, ktoré sú uvedené v modernizovanom Dohovore č. 108 a v právnych predpisoch EÚ o ochrane údajov a ktoré si vyžadujú zvýšenú ochranu, preto sa na ne vzťahuje osobitný právny režim.
- Údaje sú anonymizované, ak sa už nevzťahujú na identifikovanú alebo identifikovateľnú fyzickú osobu.
- Pseudonymizácia je opatrenie, na základe ktorého sa osobné údaje nemôžu priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, ktoré sa uchovávajú oddelene. Kľúč, ktorý umožňuje opätovnú identifikáciu dotknutých osôb, sa musí uchovávať oddelene a v bezpečí. Údaje po pseudonymizácii sú aj naďalej osobnými údajmi. V práve Únie neexistuje pojem „pseudonymizované údaje“.
- Zásady a pravidlá ochrany údajov sa nevzťahujú na anonymizované informácie. Vzťahujú sa však na pseudonymizované údaje.

2.1.1. Hlavné aspekty pojmu osobný údaj

V rámci právnych predpisov EÚ, ako aj **právnych predpisov RE**, sa „osobné údaje“ vymedzujú ako informácie, ktoré sa týkajú identifikovanej alebo identifikovateľnej fyzickej osoby¹³⁶. Ide o informácie o osobe, ktorej totožnosť je buď preukázateľne zrejmä, alebo sa dá určiť získaním doplňujúcich informácií. Na určenie toho, či je fyzická osoba identifikovateľná, by prevádzkovateľ alebo akákoľvek iná osoba mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že sa využijú na priamu alebo nepriamu identifikáciu fyzickej osoby, napríklad osobitný výber, ktorý umožňuje zaobchádzať s jednou osobou rozdielne ako s druhou¹³⁷.

Ak sa údaje takejto osoby spracúvajú, táto osoba sa nazýva „dotknutá osoba“.

Dotknutá osoba

Podľa právnych predpisov EÚ sa pravidlá ochrany údajov vzťahujú len na fyzické osoby¹³⁸ a európske právne predpisy o ochrane údajov sa vzťahujú len na žijúce osoby¹³⁹. Vo všeobecnom nariadení o ochrane údajov (GDPR) sa osobné údaje vymedzujú ako akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.

Právne predpisy RE, najmä modernizovaný Dohovor č. 108, takisto hovoria o ochrane jednotlivcov pri spracúvaní ich osobných údajov. Aj podľa nich sú osobné údaje akékoľvek informácie, ktoré sa týkajú identifikovaného alebo identifikovateľného jednotlivca. Táto fyzická osoba alebo jednotlivec, ako sa uvádza v GDPR aj v modernizovanom Dohovore č. 108, sa v právnych predpisoch o ochrane údajov nazýva dotknutá osoba.

Určitá ochrana sa vzťahuje aj na právnické osoby. V judikatúre ESĽP existujú rozsudky vo veci sťažnosti právnických osôb, ktoré sa sťažovali na údajné porušenie práva na ochranu pred použitím ich údajov podľa článku 8 ECHR. Článok 8 ECHR sa týka práva na rešpektovanie súkromného a rodinného života, ako aj

¹³⁶ Všeobecné nariadenie o ochrane údajov, článok 4 ods. 1; modernizovaný Dohovor č. 108, článok 2 písm. a).

¹³⁷ Všeobecné nariadenie o ochrane údajov, odôvodnenie 26.

¹³⁸ Tamže, článok 1.

¹³⁹ Tamže, odôvodnenie 27. Pozri tiež: Pracovná skupina zriadená podľa článku 29 (2007), *Stanovisko 4/2007 k pojmu osobné údaje*, WP 136, 20. júna 2007, s. 22.

obydlia a korešpondencie. Súd sa preto môže prípadmi zaoberať aj z hľadiska obydlia a korešpondencie, a nielen z hľadiska súkromného života.

Príklad: *Vec Bernh Larsen Holding AS a i./Nórsko*¹⁴⁰ sa týkala sťažnosti troch nórskejších spoločností na rozhodnutie daňového úradu, ktorým sa im nariaďovalo poskytnúť daňovým kontrolárom kópiu všetkých údajov z počítačového servera využívaného všetkými tromi spoločnosťami.

ESLP dospel k záveru, že takáto povinnosť uložená sťažujúcim sa spoločnostiam predstavuje zásah do ich práv, pokiaľ ide o rešpektovanie „obydlia“ a „korešpondencie“ na účely článku 8 ECHR. Súd však konštatoval, že daňové orgány mali zavedené účinné a primerané záruky proti zneužitiu: sťažujúce sa spoločnosti boli informované v dostatočnom predstihu; pri zásahu na mieste boli prítomné a mohli sa k nemu vyjadrovať; materiál sa mal po skončení daňovej kontroly zničiť. Za takýchto okolností bola dosiahnutá primeraná rovnováha medzi právom sťažujúcich sa spoločností na rešpektovanie „obydlia“ a „korešpondencie“ a ich záujmom o ochranu súkromia osôb, ktoré pre ne pracujú na jednej strane a verejným záujmom o zaistenie účinnej daňovej kontroly na strane druhej. Súd dospel k záveru, že nedošlo k žiadnemu porušeniu článku 8.

Podľa modernizovaného Dohovoru č. 108 sa ochrana údajov týka predovšetkým ochrany fyzických osôb, zmluvné strany však môžu v rámci vnútroštátnych právnych predpisov rozšíriť ochranu údajov na právnické osoby, napríklad na obchodné spoločnosti a združenia. V dôvodovej správe k modernizovanému Dohovoru sa uvádza, že vnútroštátne právne predpisy môžu chrániť oprávnené záujmy právnických osôb rozšírením rozsahu pôsobnosti Dohovoru na týchto aktérov¹⁴¹. **Právne predpisy EÚ o ochrane údajov** sa nevzťahujú na spracúvanie údajov, ktoré sa týkajú právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby¹⁴². V smernici o súkromí a elektronických komunikáciách sa však chráni dôverynosť komunikácie a oprávnené záujmy právnických osôb týkajúce sa zvyšovania kapacity automatického

140 ESLP, *Bernh Larsen Holding AS a i./Nórsko*, č. 24117/08, 14. marca 2013. Pozri tiež aj ESLP, *Liberty a i./Spojené kráľovstvo*, č. 58243/00, 1. júla 2008.

141 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 30.

142 Všeobecné nariadenie o ochrane údajov, odôvodnenie 14.

uchovávaní a spracúvaní údajov týkajúcich sa účastníkov a používateľov¹⁴³. Podobne sa v návrhu nariadenia o súkromí a elektronických komunikáciách rozširuje ochrana aj na právnické osoby.

Príklad: Vo veci *Volker und Markus Schecke a Hartmut Eifert/Land Hessen*¹⁴⁴ SDEÚ odkázal na uverejnenie osobných údajov týkajúcich sa príjemcov poľnohospodárskej pomoci a konštatoval, že „právnické osoby [sa] môžu dovolávať ochrany podľa článkov 7 a 8 Charty v súvislosti s týmto uvedením len v rozsahu, v akom názov právnickej osoby identifikuje jednu alebo viaceré fyzické osoby. [...] Dodržiavanie práva na ochranu osobného života v súvislosti so spracúvaním osobných údajov, ktoré uznávajú články 7 a 8 Charty [...], sa vzťahuje na všetky informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby [...]“¹⁴⁵.

SDEÚ zvážil na jednej strane záujem EÚ na zabezpečení transparentnosti pridelovania pomoci a na druhej strane základné práva na súkromie a ochranu údajov jednotlivcov, ktorí získali pomoc, a dospel k záveru, že zásah do týchto základných práv je neprimeraný. Domnieval sa, že cieľ zabezpečenia transparentnosti by sa mohol účinne dosiahnuť opatreniami, ktoré by menej zasahovali do práv dotknutých osôb. Pri skúmaní primeranosti zverejňovania informácií týkajúcich sa právnických osôb, ktoré dostali pomoc, však SDEÚ dospel k inému záveru, pričom rozhodol, že takéto zverejnenie neprekračuje medze zásady proporcionality. Skonštatoval, že „závažnosť zásahu do práva na ochranu osobných údajov sa totiž prejavuje inak u právnických osôb a inak u fyzických osôb“¹⁴⁶. Právnické osoby v tejto súvislosti podliehali prísnejšej povinnosti zverejnenia údajov, ktoré sa ich týkajú. SDEÚ dospel k záveru, že požiadavka, aby vnútroštátne orgány pred zverejnením údajov týkajúcich sa právnickej osoby, ktorá je prijímateľom pomoci, preskúmali, či tieto údaje identifikujú súvisiace fyzické osoby, by pre tieto orgány predstavovala neprimeranú administratívnu záťaž. V právnych predpisoch, podľa ktorých sa vyžaduje všeobecné zverejňovanie údajov týkajúcich sa právnických osôb, sa preto dosiahla spravodlivá rovnováha medzi protichodnými záujmami.

143 Smernica o súkromí a elektronických komunikáciách, odôvodnenie 7 a článok 1 ods. 2.

144 SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010, bod 53.

145 Tamže, body 52 – 53.

146 Tamže, bod 87.

Povaha údajov

Akékoľvek informácie môžu byť osobnými údajmi za predpokladu, že sa týkajú identifikovanej alebo identifikovateľnej osoby.

Príklad: Posudok pracovného výkonu zamestnanca zo strany nadriadeného, ktorý je uložený v osobnom spise zamestnanca, predstavuje osobné údaje o zamestnancovi. Platí to aj v prípade, keď čiastočne alebo úplne vyjadruje len osobný názor nadriadeného, napríklad: „zamestnanec neprejavuje pri práci nasadenie“ a neobsahuje faktické informácie, napríklad: „za posledných šesť mesiacov nebol zamestnanec päť týždňov prítomný na pracovisku“.

Osobné údaje zahŕňajú informácie týkajúce sa súkromného života osoby, ku ktorým patria aj informácie o jej pracovnej činnosti či verejnom živote.

ESLP vo veci *Amann*¹⁴⁷ vyložil pojem „osobné údaje“ tak, že nie je obmedzený na záležitosti súkromnej sféry jednotlivca. Tento význam pojmu „osobné údaje“ je preto relevantný aj pre GDPR.

Príklad: Vo veci *Volker und Markus Schecke a Hartmut Eifert/Land Hessen*¹⁴⁸ SDEÚ konštatoval, že „v tejto súvislosti nemá nijaký význam skutočnosť, že uverejňované údaje sa týkajú profesijných činností [...]. ESLP v tomto ohľade v súvislosti s výkladom článku 8 ECHR rozhodol, že pojem ‚súkromný život‘ sa nemôže vykladať reštriktívne a že žiadny principiálny dôvod neumožňuje vylúčiť profesijné činnosti... z pojmu ‚súkromný‘.“

Príklad: V spojených veciach *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*¹⁴⁹ SDEÚ skonštatoval, že právna analýza obsiahnutá v návrhu rozhodnutia oddelenia imigrácie a naturalizácie, ktoré sa zaoberá žiadosťami o povolenie na pobyt, sama osebe nepredstavuje osobné údaje, hoci môže obsahovať niektoré osobné údaje.

¹⁴⁷ Pozri ESLP, *Amann/Švajčiarsko*, č. 27798/95, 16. februára 2000, bod 65.

¹⁴⁸ SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010, bod 59.

¹⁴⁹ SDEÚ, spojené veci C-141/12 a C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*, 17. júla 2014, bod 39.

Z judikatúry ESĽP týkajúcej sa článku 8 ECHR vyplýva, že nemusí byť jednoduché úplne oddeliť záležitosti týkajúce sa súkromného a pracovného života¹⁵⁰.

Príklad: Vo veci *Bărbulescu/Rumunsko*¹⁵¹ bol sťažovateľ prepustený preto, že počas pracovného času používal internet svojho zamestnávateľa v rozpore s vnútornými predpismi. Zamestnávateľ monitoroval jeho komunikáciu a počas konania pred vnútroštátnym súdom boli predložené záznamy, ktoré obsahovali správy čisto súkromnej povahy. ESĽP dospel k záveru, že článok 8 je uplatniteľný, a ponechal tým otvorenú otázku, či reštriktívne predpisy zamestnávateľa umožnili sťažovateľovi primerané očakávanie súkromia, každopádne však konštatoval, že pokyny zamestnávateľa nemôžu obmedziť súkromný spoločenský život na pracovisku, tak aby vôbec neexistoval. Vo veci samej sa zmluvným štátom poskytla široká miera voľnej úvahy pri posudzovaní potreby vytvoriť právny rámec na úpravu podmienok, za ktorých by zamestnávateľ mohol regulovať mimopracovnú komunikáciu svojich zamestnancov – elektronickú alebo aj inú – na pracovisku. Vnútroštátne orgány však museli zabezpečiť, aby opatrenia, ktoré zamestnávateľ prijme na monitorovanie korešpondencie a inej komunikácie, bez ohľadu na ich rozsah a trvanie, boli sprevádzané primeranými a dostatočnými zárukami proti zneužitiu. Nevyhnutým prvkom bola proporionalita a procesné záruky voči vplyvu svojvoľnosti a ESĽP identifikoval viacero faktorov, ktoré boli za daných okolností relevantné. K týmto faktorom patrí napríklad rozsah monitorovania zamestnancov zo strany zamestnávateľa a stupeň narušenia súkromia zamestnanca, dôsledky pre zamestnanca a skutočnosť, či boli poskytnuté primerané záruky. Okrem toho vnútroštátne orgány museli zabezpečiť, aby zamestnanec, ktorého komunikácia bola monitorovaná, mohol podať opravný prostriedok pred súdnym orgánom s právomocou rozhodovať aspoň z vecného hľadiska o tom, ako boli uvedené kritériá dodržiavané a či boli napadnuté opatrenia zákonné. V tomto prípade ESĽP zistil porušenie článku 8, pretože vnútroštátne orgány nezabezpečili primeranú ochranu práva sťažovateľa na rešpektovanie súkromného života a korešpondencie a v dôsledku toho sa nepodarilo dosiahnuť spravodlivú rovnováhu medzi dotknutými záujmami.

150 Pozri napríklad ESĽP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000, bod 43; ESĽP, *Niemietz/Nemecko*, č. 13710/88, 16. decembra 1992, bod 29.

151 ESĽP, *Bărbulescu/Rumunsko* [VK], č. 61496/08, 5. septembra 2017, bod 121.

Podľa právnych predpisov EÚ, ako aj **právnych predpisov RE** informácie obsahujú údaje o osobe vtedy, keď:

- je jednotlivец na základe týchto informácií identifikovaný alebo identifikovateľný,
- jednotlivец, hoci nebol identifikovaný, môže byť na základe tejto informácie osobitne vybraný spôsobom, ktorý umožňuje zistiť, kto je dotknutou osobou, po vykonaní ďalšieho prieskumu.

Oba druhy informácií sú európskymi právnymi predpismi o ochrane údajov chránené rovnakým spôsobom. Priama alebo nepriama identifikovateľnosť jednotlivcov si vyžaduje nepretržité posudzovanie, pri ktorom je potrebné „zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj“¹⁵². ESLP opakovane konštatoval, že pojem „osobné údaje“ podľa ECHR je rovnaký ako v Dohovore č. 108, najmä pokiaľ ide o podmienku týkajúcu sa identifikovaných alebo identifikovateľných osôb¹⁵³.

V GDPR sa stanovuje, že fyzická osoba je identifikovateľná, keď ide o osobu, „ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby“¹⁵⁴. Identifikácia si teda vyžaduje prvky, ktoré opisujú osobu tak, že je odlišiteľná od všetkých ostatných osôb a je rozoznatelná ako jednotlivец. Základným príkladom takýchto opisných prvkov je meno osoby, ktoré môže osobu priamo identifikovať. V niektorých prípadoch môžu k podobnému výsledku viesť iné atribúty a umožniť nepriamu identifikáciu osoby. Telefónne číslo, číslo sociálneho poistenia a evidenčné číslo vozidla sú príkladmi informácií, ktoré môžu viesť k identifikácii osoby. Takisto je možné používať atribúty, ako sú počítačové súbory, súbory cookie a nástroje na sledovanie internetového prenosu, na osobitný výber osoby na základe identifikácie jej správania a zvykov. Ako sa uvádza v stanovisku pracovnej skupiny zriadenej podľa článku 29, „[b]ez toho, aby sa vôbec zisťovalo meno a adresa jednotlivca, je možné zaradiť túto osobu do kategórie na základe socioekonomických, psychologických, filozofických alebo iných kritérií a prisúdiť mu určité rozhodnutia, keďže kontaktné

152 Všeobecné nariadenie o ochrane údajov, odôvodnenie 26.

153 Pozri ESLP, *Amann/Švajčiarsko* [VK], č. 27798/95, 16. februára 2000, bod 65.

154 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 1.

miesto jednotlivca (počítača), ktoré používa, si už nutne nevyžaduje odhalenie jeho identity v užšom zmysle¹⁵⁵. Vymedzenie osobných údajov v rámci RE aj EÚ je dostatočne široké na to, aby zahŕňalo všetky možnosti identifikácie (a teda aj všetky stupne identifikovateľnosti).

Príklad: SDEÚ vo veci *Promusicae/Telefónica de España*¹⁵⁶ konštatoval, že sa nespochybňuje, že „oznámenie mien a adries určitých užívateľov programu [určitá internetová platforma na výmenu súborov], ktorého sa domáha Promusicae, znamená sprístupnenie osobných údajov, t. j. informácií o identifikovaných alebo identifikovateľných fyzických osobách v súlade s definíciou uvedenou v článku 2 písm. a) smernice 95/46 [v súčasnosti článok 4 ods. 1 GDPR]. Toto oznámenie informácií, ktoré sú podľa združenia Promusicae uchovávané spoločnosťou Telefónica, čo táto spoločnosť nepopiera, predstavuje spracúvanie osobných údajov“¹⁵⁷.

Príklad: Vec *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*¹⁵⁸ sa týkala toho, že poskytovateľ internetových služieb, spoločnosť Scarlet, odmietla nainštalovať systém na filtrovanie elektronických komunikácií, ktoré používajú softvér na výmenu súborov, s cieľom zabrániť výmene súborov, ktorá porušuje autorské práva chránené organizáciou SABAM, zväzom kolektívnej správy práv, ktorý zastupuje autorov, skladateľov a vydavateľov. SDEÚ rozhodol, že IP adresy „predstavujú chránené osobné údaje, pretože umožňujú presnú identifikáciu uvedených používateľov“.

Keďže mnohé mená nie sú jedinečné, určenie totožnosti osoby si môže vyžadovať dodatočné atribúty na zabezpečenie toho, že osoba nebude mylne považovaná za nejakú inú osobu. Niekedy môže byť potrebné skombinovať priame a nepriame atribúty, aby bolo možné identifikovať osobu, ktorej sa informácie týkajú. Často sa používa deň a miesto narodenia. Okrem toho sa v niektorých krajinách na lepšie

155 Pracovná skupina zriadená podľa článku 29, *Stanovisko 4/2007 k pojmu osobné údaje*, WP 136, 20. júna 2007, s. 15.

156 SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [VK], 29. januára 2008, bod 45.

157 Predtým smernica 95/46, článok 2 písm. b), teraz všeobecné nariadenie o ochrane údajov, článok 4 ods. 2.

158 SDEÚ, C-70/10, *Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)*, 24. novembra 2011, bod 51.

rozlišovanie občanov zaviedli osobné čísla. Prenesené daňové údaje¹⁵⁹, údaje týkajúce sa žiadateľa o povolenie na pobyt obsiahnuté v správnom dokumente¹⁶⁰ a dokumenty týkajúce sa bankových a fiduciárnych vzťahov¹⁶¹ môžu predstavovať osobné údaje. V technologickom veku sa na identifikáciu osôb čoraz častejšie používajú biometrické údaje, ako sú odtlačky prstov, digitálne fotografie alebo snímky očnej dúhovky, ako aj lokalizačné údaje a online charakteristiky.

V prípade uplatniteľnosti európskych právnych predpisov o ochrane údajov nie je potrebná skutočná identifikácia dotknutej osoby; stačí, že táto dotknutá osoba je identifikovateľná. Osoba sa považuje za identifikovateľnú, ak je k dispozícii dostatok prvkov, prostredníctvom ktorých môže byť osoba priamo alebo nepriamo identifikovaná¹⁶². Podľa odôvodnenia 26 GDPR spočíva kritérium v tom, či je alebo nie je pravdepodobné, že k dispozícii budú primerané prostriedky na identifikáciu a predvídateľní používatelia informácií; patria sem informácie uchovávané príjemcami tretích strán (pozri [oddiel 2.3.2](#)).

Príklad: Miestny orgán sa rozhodol, že začne zbierať údaje o prekročení povolennej rýchlosti vozidlami na miestnych uliciach. Fotografuje vozidlá a automaticky zaznamenáva čas a miesto s cieľom postúpiť tieto údaje príslušnému orgánu, aby mohol pokutovať vodičov, ktorí porušili obmedzenie rýchlosti. Dotknutá osoba predložila sťažnosť, podľa ktorej miestny úrad nemá na takýto zber údajov žiadny právny základ v právnych predpisoch o ochrane údajov. Miestny orgán namieta, že nezbiera osobné údaje. Evidenčné čísla vozidiel sú podľa jeho názoru anonymnými údajmi. Miestny orgán nemá žiadne oprávnenie na prístup do všeobecného registra motorových vozidiel na účely zistenia totožnosti vlastníka vozidla alebo vodiča.

Toto odôvodnenie nie je v súlade s odôvodnením 26 GDPR. Keďže účelom zberu údajov je preukázateľne identifikácia a pokutovanie vodičov, ktorí prekročia predpísanú rýchlosť, predpokladá sa teda snaha o identifikáciu osôb. Aj keď miestne orgány nemajú prostriedky na priamu identifikáciu, postúpia údaje príslušnému orgánu, teda polícii, ktorá takéto prostriedky

159 SDEÚ, C-201/14, *Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*, 1. októbra 2015.

160 SDEÚ, *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*, 17. júla 2014.

161 ESLP, *M.N. a i./San Marino*, č. 28005/12, 7. júla 2015.

162 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 1.

má. V odôvodnení 26 je takisto výslovne zahrnutá situácia, v ktorej je možné predpokladať, že ďalší príjemcovia údajov (iní ako bezprostredný používateľ údajov) sa môžu pokúsiť o identifikáciu jednotlivcov. Z hľadiska odôvodnenia 26 je činnosť miestneho orgánu rovnocenná so zberom údajov o identifikovateľných osobách, a preto si vyžaduje právny základ v právnych predpisoch o ochrane údajov.

Na „zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj“¹⁶³.

Príklad: Vo veci *Breyer/Bundesrepublik Deutschland*¹⁶⁴ sa SDEÚ zaoberal pojmom nepriama identifikovateľnosť dotknutých osôb. Vec sa týkala dynamických IP adries, ktoré sa menia pri každom novom pripojení k internetu. Webové sídla, ktoré prevádzkujú nemecké spolkové orgány, registrujú a uchovávajú dynamické IP adresy, aby predchádzali kybernetickým útokom a aby v prípade potreby mohli začať trestné konania. Len poskytovateľ internetových služieb, ktorého služby pán Breyer využíval, mal dodatočné informácie potrebné na jeho identifikáciu.

SDEÚ dospel k záveru, že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva, keď si určitá osoba prehliada internetovú stránku, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje osobné údaje aj napriek tomu, že ďalšie informácie potrebné na identifikáciu tejto osoby má k dispozícii len tretí subjekt, v tomto prípade jej poskytovateľ internetového pripojenia¹⁶⁵. Konštatoval, že na to, aby informácie predstavovali osobné údaje, „nie je nevyhnutné, aby sa všetky informácie umožňujúce identifikovať dotknutú osobu museli nachádzať v rukách jednej osoby“. Používatelia dynamickej IP adresy, ktorú registruje poskytovateľ internetového pripojenia, môžu byť v určitých situáciách, napríklad v rámci trestného konania v prípade kybernetických útokov, identifikovaní s pomocou iných osôb¹⁶⁶.

¹⁶³ Tamže, odôvodnenie 26.

¹⁶⁴ SDEÚ, C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19. októbra 2016, body 47 – 48.

¹⁶⁵ Predtým smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe týchto údajov, článok 2 písm. a).

¹⁶⁶ SDEÚ, C-70/10, *Scarlet Extended SA/Société belge des auteurs compositeurs et éditeurs (SABAM)*, 24. novembra 2011, body 47 – 48.

Podľa SDEÚ, ak poskytovateľ „má k dispozícii právne prostriedky, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby“, predstavuje to „prostriedok, ktorý môže byť rozumne použitý pre identifikáciu dotknutej osoby“. Takéto údaje sa preto považujú za osobné údaje.

Právne predpisy RE identifikovateľnosť chápu podobne. V dôvodovej správe k modernizovanému Dohovoru č. 108 je uvedený podobný opis: pojem „identifikovateľný“ sa nevzťahuje len na občiansku alebo právnu identitu osoby ako takej, ale aj na to, čo môže viesť k tomu, že konkrétna osoba bude „individualizovaná“ alebo osobitne vybraná spomedzi ostatných a v dôsledku toho sa s ňou bude zaobchádzať odlišne. Takáto „individualizácia“ by sa mohla vykonať napríklad konkrétnym odkazom na osobu alebo na zariadenie či súbor zariadení (počítač, mobilný telefón, fotoaparát, hracie zariadenia atď.), ktoré sa spájajú s identifikačným číslom, s pseudonymom, biometrickými alebo genetickými údajmi, lokalizačnými údajmi, IP adresou alebo iným identifikátorom¹⁶⁷. Jednotlivec sa nepovažuje za „identifikovateľného“, ak si jeho identifikácia vyžaduje vynaloženie neprimeraného času, úsilia alebo zdrojov. Ide napríklad o situáciu, keď by si identifikácia dotknutej osoby vyžadovala príliš zložitú, dlhú a nákladnú činnosť. Neprimeranosť času, úsilia alebo zdrojov sa musí posudzovať v každom prípade individuálne, pričom sa zohľadňujú faktory, ako je účel spracúvania, náklady a výhody identifikácie, druh prevádzkovateľa a použitá technológia¹⁶⁸.

Pokiaľ ide o formu, v akej sa osobné údaje uchovávali alebo používajú, je dôležité uviesť, že z hľadiska uplatniteľnosti právnych predpisov o ochrane údajov nie je relevantná. Písomná alebo ústna komunikácia môže obsahovať osobné údaje, ako aj obrázky¹⁶⁹ vrátane nahrávok z kamerového systému¹⁷⁰ alebo zvuk¹⁷¹. Elektronicky zaznamenané informácie a informácie v papierovej forme môžu byť tiež osobnými údajmi. Dokonca aj bunkové vzorky ľudského tkaniva – v ktorých je zaznamenaná

167 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 18.

168 Tamže, bod 17.

169 ESLP, *Von Hannover/Nemecko*, č. 59320/00, 24. júna 2004; ESLP, *Sciacca/Taliansko*, č. 50774/99, 11. januára 2005; SDEÚ, C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11. decembra 2014.

170 ESLP, *Peck/Spojené kráľovstvo*, č. 44647/98, 28. januára 2003; ESLP, *Köpke/Nemecko* (rozh.), č. 420/07, 5. októbra 2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17. marca 2010.

171 ESLP, *P.G. a J.H./Spojené kráľovstvo*, č. 44787/98, 25. septembra 2001, body 59 – 60; ESLP, *Wisse/Francúzsko*, č. 71611/01, 20. decembra 2005 (francúzske znenie).

DNA osoby – môžu byť zdrojmi, z ktorých sa môžu získať biometrické údaje¹⁷², pokiaľ sa údaje týkajú zdedených alebo získaných genetických charakteristík osoby, poskytujú jedinečné informácie o jej zdraví alebo fyziológii a vyplývajú z analýzy biologickej vzorky od tejto osoby¹⁷³.

Anonymizácia

Podľa zásady minimalizácie uchovávaní údajov, ktorá je obsiahnutá v GDPR, ako aj v modernizovanom Dohovore č. 108 (podrobnejšie sa rozoberá v kapitole 3), sa údaje musia uchovávať „vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú“¹⁷⁴. Z toho vyplýva, že údaje by sa museli vymazať alebo anonymizovať, ak by ich prevádzkovateľ chcel uchovávať po tom, čo už viac nie sú potrebné a prestali slúžiť svojmu pôvodnému účelu.

Proces anonymizácie údajov znamená, že všetky identifikačné prvky sú odstránené zo súboru osobných údajov, takže dotknutá osoba už nie je identifikovateľná¹⁷⁵. Pracovná skupina zriadená podľa článku 29 vo svojom stanovisku 05/2014 analyzuje účinnosť a obmedzenia rôznych techník anonymizácie¹⁷⁶. Uznáva sa potenciálna hodnota takýchto techník, ale zdôrazňuje sa, že určité techniky nemusia nevyhnutne fungovať vo všetkých prípadoch. Nájdenie optimálneho riešenia v danej situácii si vyžaduje, aby sa o vhodnom procese anonymizácie rozhodovalo na individuálnom základe. Bez ohľadu na použitú techniku je potrebné nezvratne zabrániť identifikácii. To znamená, že v prípade anonymizácie údajov sa v informáciách nesmie ponechať žiadny prvok, ktorý by pri vynaložení primeraného úsilia mohol slúžiť na opätovné identifikovanie dotknutej osoby (dotknutých osôb)¹⁷⁷. Riziko opätovnej identifikácie možno posúdiť tak, že sa zohľadní „čas, úsilie alebo zdroje potrebné vzhľadom na

172 Pozri dokument pracovnej skupiny zriadenej podľa článku 29 (2007), *Stanovisko 4/2007 k pojmu osobné údaje*, WP136, 20. júna 2007, s. 9; Rada Európy, odporúčanie Rec(2006)4 Výboru ministrov členským štátom v oblasti výskumu na biologických materiáloch ľudského pôvodu, 15. marca 2006.

173 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 13.

174 Tamže, článok 5 ods. 1 písm. e); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. e).

175 Všeobecné nariadenie o ochrane údajov, odôvodnenie 26.

176 Pracovná skupina zriadená podľa článku 29 (2014), *Stanovisko 5/2014 k technikám anonymizácie*, WP216, 10. apríla 2014.

177 Všeobecné nariadenie o ochrane údajov, odôvodnenie 26.

povahu údajov, kontext ich použitia, dostupné technológie na opätovnú identifikáciu a súvisiace náklady”¹⁷⁸.

Po úspešnej anonymizácii údajov už tieto údaje nie sú osobnými údajmi a právne predpisy na ochranu údajov sa už na ne nevzťahujú.

V GDPR sa stanovuje, že osoba alebo organizácia, ktorá je prevádzkovateľom vo vzťahu k spracúvaniu osobných údajov, nemôže byť povinná uchovávať, získať alebo spracúvať dodatočné informácie na identifikáciu dotknutej osoby výlučne na dosiahnutie súladu s týmto nariadením. Toto pravidlo má však významnú výnimku: ak dotknutá osoba pri výkone svojho práva na prístup, opravu, vymazanie, obmedzenie spracúvania a prenosnosť údajov, poskytne dodatočné informácie, ktoré umožňujú jej identifikáciu, údaje, ktoré sa predtým anonymizovali, sa stanú opäť osobnými údajmi¹⁷⁹.

Pseudonymizácia

Osobné informácie obsahujú atribúty, ako je meno, dátum narodenia, pohlavie, adresu alebo iné prvky, ktoré by mohli viesť k identifikácii. Proces pseudonymizácie osobných údajov znamená, že tieto atribúty sa nahrádzajú pseudonymom.

V **právnych predpisoch** EÚ sa „pseudonymizácia“ vymedzuje ako „spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe”¹⁸⁰. Na rozdiel od anonymizovaných údajov sú pseudonymizované údaje stále osobnými údajmi, a preto podliehajú právnym predpisom o ochrane údajov. Hoci pseudonymizácia môže znížiť bezpečnostné riziká pre dotknuté osoby, nie je vyňatá z rozsahu pôsobnosti GDPR.

Podľa GDPR sa uznávajú rôzne spôsoby pseudonymizácie ako vhodné technické opatrenia na zvýšenie ochrany údajov a pseudonymizácia sa osobitne spomína

178 Rada Európy, Výbor pre Dohovor č. 108 (2017), *Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big Data*, 23. januára 2017, bod 6.2.

179 Všeobecné nariadenie o ochrane údajov, článok 11.

180 Tamže, článok 4 ods. 5.

pri ich navrhovaní a bezpečnosti spracúvaných údajov¹⁸¹. Takisto ide o primeranú záruku, ktorá by sa mohla použiť pri spracúvaní osobných údajov na iné účely, než na ktoré boli pôvodne získané¹⁸².

Pseudonymizácia sa v právnych vymedzeniach pojmov modernizovaného Dohovoru **RE** č. 108 výslovne neuvádza. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa však jasne uvádza, že „používanie pseudonymu alebo akéhokoľvek digitálneho identifikátora/digitálnej identity nevedie k anonymizácii údajov, keďže dotknutá osoba môže byť ešte identifikovateľná alebo individualizovaná“¹⁸³. Jedným zo spôsobov pseudonymizácie údajov je šifrovanie údajov. Po vykonaní pseudonymizácie údajov existuje prepojenie s totožnosťou vo forme pseudonymu plus dešifrovacieho kľúča. Bez takéhoto kľúča je pseudonymizované údaje ťažké identifikovať. Osoby oprávnené používať dešifrovací kľúč však opätovnú identifikáciu vykonajú ľahko. Dešifrovacie kľúče sa musia osobitne chrániť pred používaním neoprávnenými osobami. Z tohto dôvodu sa „[p]seudonymizované údaje [...] považujú za osobné údaje [...]“, na ktoré sa vzťahuje modernizovaný Dohovor č. 108¹⁸⁴.

Autentifikácia

Ide o postup, prostredníctvom ktorého je osoba schopná dokázať, že má určitú totožnosť a/alebo je oprávnená vykonať určité činnosti, napríklad vstúpiť do bezpečnostnej zóny alebo vyzdvihnúť peniaze z bankového účtu. Autentifikácia sa môže uskutočniť formou porovnania biometrických údajov, napríklad fotografie alebo odtlačkov prstov v cestovnom pase, s údajmi osoby, ktorá sa predstavuje napríklad pri imigračnej kontrole¹⁸⁵. Ďalším prostriedkom autentifikácie je žiadosť o uvedenie informácií, ktoré by mala poznať len osoba s určitou totožnosťou alebo poverením, napríklad osobného identifikačného čísla (PIN) alebo hesla, alebo požiadanie o predloženie určitého tokenu, ktorý by mala vlastniť výlučne osoba s určitou totožnosťou alebo poverením, napríklad špeciálnej čipovej karty alebo kľúča k bankovému trezoru. Medzi mimoriadne účinné nástroje na identifikáciu a autentifikáciu osoby v rámci elektronickej komunikácie patria okrem hesiel alebo čipových kariet aj elektronické podpisy niekedy spojené s PIN kódom.

181 Tamže, článok 25 ods. 1.

182 Tamže, článok 6 ods. 4.

183 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 18.

184 Tamže.

185 Tamže, body 56 – 57.

2.1.2. Osobitné kategórie osobných údajov

V rámci právnych predpisov EÚ, ako aj právnych predpisov RE existujú osobitné kategórie osobných údajov, ktoré vzhľadom na svoju povahu môžu pri spracúvaní predstavovať riziko pre dotknuté osoby a vyžadujú si zvýšenú ochranu. Na tieto údaje sa vzťahuje zásada zákazu a existuje obmedzený počet podmienok, pri ktorých je ich spracúvanie zákonné.

V rámci modernizovaného Dohovoru č. 108 (článok 6) a GDPR (článok 9) sa za citlivé údaje považujú tieto kategórie:

- osobné údaje odhalujúce rasový alebo etnický pôvod,
- osobné údaje odhalujúce politické názory, náboženské alebo filozofické presvedčenie,
- osobné údaje odhalujúce členstvo v odborových organizáciách,
- genetické údaje a biometrické údaje spracúvané na účel identifikácie osoby,
- osobné údaje týkajúce sa zdravia, sexuálneho života alebo sexuálnej orientácie.

Príklad: Vec *Bodil Lindquist*¹⁸⁶ sa týkala odkazovania na rôzne osoby prostredníctvom ich mena alebo iným spôsobom, napríklad na základe ich telefónneho čísla alebo informácií o ich záľubách, na internetovej stránke. SDEÚ konštatoval, že „údaj o tom, že si určitá osoba poranila nohu a je čiastočne práceneschopná, je osobným údajom týkajúcim sa zdravia“¹⁸⁷.

Osobné údaje týkajúce sa uznania viny za trestné činy a priestupky

Podľa modernizovaného Dohovoru č. 108 sa do zoznamu osobitných kategórií osobných údajov zahŕňajú aj osobné údaje týkajúce sa priestupkov, trestných konaní a trestných činov a súvisiacich bezpečnostných opatrení¹⁸⁸. V rámci GDPR sa osobné údaje týkajúce sa uznania viny za trestné činy a priestupky alebo súvisiacich

¹⁸⁶ SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003, bod 51.

¹⁸⁷ Predtým smernica 95/46, článok 8 ods. 1, teraz všeobecné nariadenie o ochrane údajov, článok 9 ods. 1.

¹⁸⁸ Modernizovaný Dohovor č. 108, článok 6 ods. 1.

bezpečnostných opatrení ako také neuvádzajú v zozname osobitných kategórií údajov, ale sú predmetom samostatného článku. V článku 10 GDPR sa stanovuje, že spracúvanie takýchto údajov sa môže vykonávať len „pod kontrolou orgánu verejnej moci, alebo ak je spracúvanie povolené právom Únie alebo právom členského štátu poskytujúcim primerané záruky ochrany práv a slobôd dotknutých osôb“. Komplexné registre informácií o odsúdeniach za trestné činy môžu byť vedené len pod kontrolou osobitných orgánov verejnej moci¹⁸⁹. V EÚ sa spracúvanie osobných údajov v súvislosti s presadzovaním práva riadi osobitným právnym nástrojom, ktorým je smernica (EÚ) 2016/680¹⁹⁰. V smernici sa stanovujú osobitné pravidlá ochrany údajov, ktoré sú záväzné pre príslušné orgány, keď spracúvajú osobné údaje konkrétne na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania (pozri [oddiel 8.2.1](#)).

2.2. Spracúvanie údajov

Hlavné body

- „Spracúvanie údajov“ sa týka každej operácie vykonávanej s osobnými údajmi.
- Pojem „spracúvanie“ zahŕňa automatizované a neautomatizované spracúvanie.
- Podľa právnych predpisov EÚ sa „spracúvanie“ týka aj manuálneho spracúvania v štruktúrovaných informačných systémoch.
- Podľa právnych predpisov RE možno význam pojmu „spracúvanie“ rozšíriť v rámci vnútroštátnej právnej úpravy s cieľom zahrnúť manuálne spracúvanie.

2.2.1. Konceptia spracúvania údajov

Spracúvanie osobných údajov predstavuje komplexnú koncepciu **v právnych predpisoch EÚ, ako aj RE**: „spracúvanie osobných údajov“ [...] je operácia [...], napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo

¹⁸⁹ Všeobecné nariadenie o ochrane údajov, článok 10.

¹⁹⁰ Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, ú. v. EÚ L 119, 2016.

kombinovanie, obmedzenie, vymazanie alebo likvidácia”¹⁹¹ osobných údajov. V modernizovanom Dohovore č. 108 sa do tohto vymedzenia pojmu dopĺňa uchovávanie osobných údajov¹⁹².

Príklad: Vo veci *František Ryneš*¹⁹³ pán Ryneš domácim kamerovým systémom, ktorý nainštaloval na ochranu svojho majetku, zaznamenal obraz dvoch osôb, ktoré rozbili okná na jeho dome. SDEÚ konštatoval, že kamerový systém, ktorý zahŕňa zaznamenávanie a uchovávanie osobných údajov, predstavuje automatické spracúvanie údajov, ktoré patrí do rozsahu pôsobnosti právnych predpisov EÚ o ochrane údajov.

Príklad: Vo veci *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*¹⁹⁴ pán Manni požiadal o vymazanie svojich osobných údajov z registra ratingovej spoločnosti, ktoré ho spájajú s likvidáciou realitnej spoločnosti, pričom to negatívne ovplyvňuje jeho dobré meno. SDEÚ skonštatoval, že „zapisovaním a uchovávaním uvedených informácií v registri a prípadným ich poskytnutím na požiadanie tretím osobám orgán zodpovedný za vedenie tohto registra ‚spracúva osobné údaje‘, za ktorých spracovanie je ‚zodpovedný‘“.

Príklad: Zamestnávateľia získavajú a spracúvajú údaje o svojich zamestnancoch vrátane informácií týkajúcich sa miezd. Právnym základom pre zákonnosť tejto činnosti sú pracovné zmluvy.

Zamestnávateľia musia zasielať údaje o mzdách svojich zamestnancov daňovému úradu. Toto zasielanie údajov je takisto „spracúvaním“ v zmysle tohto pojmu v modernizovanom Dohovore č. 108 a v GDPR. Právnym základom takéhoto poskytovania však nie sú pracovné zmluvy. Pre spracovateľské operácie, ktoré vedú k poskytovaniu údajov o mzdách od zamestnávateľa daňovému úradu, musí existovať dodatočný právny základ. Tento právny základ

¹⁹¹ Všeobecné nariadenie o ochrane údajov, článok 4 ods. 2. Pozri aj modernizovaný Dohovor č. 108, článok 2 písm. b).

¹⁹² Modernizovaný Dohovor č. 108, článok 2 písm. b).

¹⁹³ SDEÚ, C-212/13, *František Ryneš/Úrad pro ochranu osobních údajů*, 11. decembra 2014, bod 25.

¹⁹⁴ SDEÚ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9. marca 2017 bod 35.

sa zvyčajne nachádza v ustanoveniach vnútroštátnych daňových predpisov. Bez takýchto ustanovení – a bez akéhokoľvek iného legitímneho dôvodu na spracúvanie – by bolo toto poskytnutie údajov nezákonným spracúvaním.

2.2.2. Automatizované spracúvanie údajov

Ochrana údajov v rámci modernizovaného Dohovoru č. 108 a GDPR sa v plnej miere vzťahuje na automatizované spracúvanie údajov.

Podľa **právnych predpisov EÚ** sa automatizované spracúvanie údajov vzťahuje na operácie vykonávané s „osobnými údajmi úplne alebo čiastočne automatizovanými prostriedkami“¹⁹⁵. Modernizovaný Dohovor č. 108 obsahuje podobnú definíciu¹⁹⁶. Z praktického hľadiska to znamená, že akékoľvek spracúvanie osobných údajov automatizovanými prostriedkami s pomocou napríklad osobného počítača, mobilného zariadenia alebo routera podlieha pravidlám EÚ a RE na ochranu údajov.

Príklad: Vec *Bodil Lindqvist*¹⁹⁷ sa týkala odkazovania na internetovej stránke na rôzne osoby prostredníctvom ich mena alebo iným spôsobom, napríklad na základe ich telefónneho čísla alebo informácií o ich záľubách. SDEÚ konštatoval, že „operácia, ktorou sa odkazuje na internetovej stránke, na rôzne osoby a ktorou sa tieto osoby identifikujú buď prostredníctvom ich mena, alebo iným spôsobom, napríklad prostredníctvom ich telefónneho čísla alebo informácií o ich pracovných podmienkach a o ich záľubách, predstavuje „úplne alebo čiastočne automatizované spracovanie osobných údajov““ v zmysle článku 3 ods. 1 smernice 95/46¹⁹⁸.

Príklad: Vo veci *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*¹⁹⁹ pán González požiadal o odstránenie alebo zmenu odkazu, na základe ktorého sa po zadaní jeho mena vo vyhľadávачi Google zobrazí odkaz na dve stránky denníka, ktoré obsahujú oznámenia o dražbe nehnuteľností z dôvodu vymáhania dlhov v oblasti

195 Všeobecné nariadenie o ochrane údajov, článok 2 ods. 1 a článok 4 ods. 2.

196 Modernizovaný Dohovor č. 108, článok 2 písm. b a c); dôvodová správa k modernizovanému Dohovoru č. 108, ods. 21.

197 SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003, bod 27.

198 Všeobecné nariadenie o ochrane údajov, článok 2 ods. 1.

199 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014.

sociálneho zabezpečenia. SDEÚ skonštatoval, že „automatickým, neustálym a systematickým preskúvaním internetu na účely hľadania informácií, ktoré sú tam uverejnené, poskytovateľ vyhľadávača ,zbiera‘ takéto údaje, ktoré následne ,vyhľadáva‘, ,zaznamenáva‘ a ,organizuje‘ v rámci svojich indexačných programov, ,uschováva‘ na svojich serveroch a prípadne ,odhaľuje‘ a ,sprístupňuje‘ svojim používateľom vo forme zoznamov výsledkov ich vyhľadávanií“²⁰⁰. SDEÚ dospel k záveru, že takéto opatrenia predstavujú „spracúvanie“, „pričom je irelevantné, že poskytovateľ vyhľadávača uplatňuje rovnaké operácie aj na iný druh informácií a nerozlišuje medzi týmito informáciami a osobnými údajmi“.

2.2.3. Neautomatizované spracúvanie údajov

Manuálne spracúvanie údajov si takisto vyžaduje ochranu údajov.

Ochrana údajov **podľa právnych predpisov EÚ** rozhodne nie je obmedzená len na automatizované spracúvanie údajov. Podľa právnych predpisov EÚ sa ochrana údajov vzťahuje na spracúvanie osobných údajov v manuálnom informačnom systéme, teda v osobitne štruktúrovanom papierovom spise²⁰¹. Štruktúrovaný informačný systém je taký systém, v ktorom sa kategorizuje súbor osobných údajov tak, že je prístupný podľa určitých kritérií. Napríklad, ak zamestnávateľ vedie papierový spis s názvom „pracovné voľno zamestnancov“, ktorý obsahuje všetky údaje o pracovnom voľne, ktoré zamestnanci v uplynulom roku vyčerpali, a je zoradený v abecednom poradí, spis bude predstavovať manuálny informačný systém podliehajúci pravidlám EÚ na ochranu údajov. Dôvodom takéhoto rozšírenia ochrany údajov je skutočnosť, že:

- papierové spisy môžu byť štruktúrované spôsobom, ktorý umožňuje rýchle a ľahké vyhľadávanie informácií,
- uchovávanie osobných údajov v štruktúrovaných papierových spisoch uľahčuje obchádzanie obmedzení stanovených zákonom pri automatizovanom spracúvaní údajov²⁰².

200 Tamže, bod 28.

201 Všeobecné nariadenie o ochrane údajov, článok 2 ods. 1.

202 Všeobecné nariadenie o ochrane údajov, odôvodnenie 15.

V **právnych predpisoch RE** sa pri vymedzení pojmu automatické spracúvanie uznáva, že medzi automatizovanými operáciami sa môžu vyžadovať určité fázy manuálneho používania osobných údajov²⁰³. V článku 2 písm. c) modernizovaného Dohovoru č. 108 sa uvádza, že „ak sa nepoužíva automatizované spracúvanie, spracúvanie údajov znamená operáciu alebo súbor operácií, ktoré sa vykonávajú s osobnými údajmi v rámci štruktúrovaného súboru takýchto údajov, ktoré sú dostupné alebo ktoré možno získať na základe špecifických kritérií“.

2.3. Používatelia osobných údajov

Hlavné body

- Každý, kto určuje účely a prostriedky spracúvania osobných údajov iných, je podľa právnych predpisov o ochrane údajov „prevádzkovateľom“. Ak takéto rozhodnutie prijme spoločne niekoľko osôb, môžu sa stať „spoločnými prevádzkovateľmi“.
- „Sprostredkovateľ“ je fyzická alebo právnická osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa.
- Sprostredkovateľ sa stáva prevádzkovateľom vtedy, ak sám určuje účely a prostriedky spracúvania údajov.
- Každý, kto prijíma údaje od prevádzkovateľa, je „prijemca“.
- „Tretia strana“ je fyzická alebo právnická osoba iná než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.
- Súhlas ako právny základ na spracúvanie osobných údajov musí byť slobodne daný, informovaný, konkrétny a jednoznačný prejav vôle s jednoznačným potvrdzujúcim úkonom vyjadrujúcim súhlas so spracúvaním.
- Spracúvanie osobitných kategórií údajov na základe súhlasu si vyžaduje výslovný súhlas.

2.3.1. Prevádzkovatelia a sprostredkovatelia

Najzávažnejším dôsledkom postavenia prevádzkovateľa alebo sprostredkovateľa je právna zodpovednosť za plnenie príslušných povinností vyplývajúcich z právnych predpisov o ochrane údajov. V súkromnom sektore zvyčajne ide o fyzickú alebo

²⁰³ Modernizovaný Dohovor č. 108, článok 2 písm. b) a c).

právnickú osobu, vo verejnom sektore je to spravidla orgán. Medzi prevádzkovateľom a sprostredkovateľom existuje zásadný rozdiel: prevádzkovateľ je fyzická alebo právnická osoba, ktorá určuje účely a prostriedky spracúvania, zatiaľ čo sprostredkovateľ je fyzická alebo právnická osoba, ktorá spracúva údaje v mene prevádzkovateľa podľa jeho presných pokynov. V zásade je to prevádzkovateľ, ktorý musí mať kontrolu nad spracúvaním a ktorý nesie zodpovednosť za spracúvanie vrátane právnej zodpovednosti. Po reforme pravidiel ochrany údajov sú však už aj sprostredkovatelia povinní plniť mnohé z požiadaviek, ktoré sa vzťahujú na prevádzkovateľov. Napríklad podľa GDPR musia sprostredkovatelia viesť záznamy o všetkých kategóriách spracovateľských činností, aby preukázali, že plnia svoje povinnosti vyplývajúce z tohto nariadenia²⁰⁴. Sprostredkovatelia sú tiež povinní zaviesť primerané technické a organizačné opatrenia s cieľom zaistiť bezpečnosť spracúvania²⁰⁵, v určitých situáciách určiť zodpovednú osobu²⁰⁶ a oznámiť porušenia ochrany údajov prevádzkovateľovi²⁰⁷.

Skutočnosť, či je osoba spôsobilá rozhodovať a určovať účel a prostriedky spracúvania, závisí od konkrétnych skutočností alebo okolností prípadu. Podľa vymedzenia pojmu prevádzkovateľ v GDPR môžu byť prevádzkovateľom fyzické osoby, právnické osoby alebo akékoľvek iné subjekty. Pracovná skupina zriadená podľa článku 29 však zdôraznila, že na to, aby sa jednotlivcom zabezpečil stabilnejší subjekt na uplatňovanie ich práv v rámci smernice, „by sa mala za prevádzkovateľa skôr považovať spoločnosť alebo orgán ako taký než konkrétna osoba v rámci spoločnosti alebo orgánu“²⁰⁸. Napríklad, ak spoločnosť predáva zdravotnícke potreby odborníkom z praxe, prevádzkovateľom je táto spoločnosť, pokiaľ ide o zostavovanie a vedenie distribučného zoznamu všetkých odborníkov v určitej oblasti, a nie vedúci predaja, ktorý tento zoznam skutočne používa a vedie.

Príklad: Ak marketingové oddelenie spoločnosti Sunshine naplánuje, že bude spracúvať údaje na účely prieskumu trhu, prevádzkovateľom pri tomto spracúvaní nebudú zamestnanci marketingového oddelenia, ale spoločnosť Sunshine. Marketingové oddelenie nemôže byť prevádzkovateľom, pretože nemá žiadnu samostatnú právnu subjektivitu.

204 Všeobecné nariadenie o ochrane údajov, článok 30 ods. 2.

205 Tamže, článok 32.

206 Tamže, článok 37.

207 Tamže, článok 33 ods. 2.

208 Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010.

Fyzické osoby môžu byť prevádzkovateľmi podľa práva Únie, ako aj práva RE. Pri spracúvaní údajov o iných osobách v kontexte výlučne osobnej alebo domácej činnosti sa však na súkromné osoby nevzťahujú ustanovenia GDPR a modernizovaného Dohovoru č. 108 a nepovažujú sa za prevádzkovateľov²⁰⁹. Osoba ktorá vedie vlastnú korešpondenciu, osobný denník opisujúci udalosti s priateľmi a kolegami a zdravotné záznamy rodinných príslušníkov, môže byť vyňatá z pravidiel ochrany údajov, pretože pri týchto činnostiach by mohlo ísť o výlučne osobné alebo iba domáce činnosti. V GDPR sa ďalej uvádza, že osobné alebo domáce činnosti by mohli zahŕňať aj využívanie sociálnych sietí a online činnosti vykonávané v kontexte takýchto činností²¹⁰. Naopak, pravidlá ochrany údajov sa v plnom rozsahu uplatňujú na prevádzkovateľov alebo sprostredkovateľov, ktorí poskytujú prostriedky na spracúvanie osobných údajov na takéto osobné alebo domáce činnosti (napríklad platformy sociálnych sietí)²¹¹.

Prístup občanov na internet a ich možnosť využívať platformy elektronického obchodu, sociálne siete a blogové stránky na výmenu osobných informácií o sebe a iných jednotlivcoch čoraz viac sťažujú oddelovanie spracúvania na osobné účely od ostatného spracúvania²¹². To, či sú činnosti výlučne osobného alebo domáceho charakteru, závisí od okolností²¹³. Na činnosti, ktoré majú profesijný alebo komerčný aspekt, sa nemôže vzťahovať výnimka pre domáce činnosti²¹⁴. Preto, ak z rozsahu a frekvencie spracúvania údajov vyplýva, že ide o profesijnú činnosť alebo činnosť na plný úväzok, súkromná osoba by sa mala považovať za prevádzkovateľa. Okrem profesijnej alebo komerčnej povahy spracovateľskej činnosti je ďalším faktorom, ktorý sa má zohľadniť, skutočnosť, či sa osobné údaje sprístupňujú veľkému počtu osôb, zjavne mimo súkromnej sféry jednotlivca. V judikatúre podľa smernice o ochrane údajov sa konštatuje, že právne predpisy na ochranu údajov sa budú uplatňovať vtedy, ak súkromná osoba pri používaní internetu uverejňuje údaje o iných na verejnom webovom sídle. SDEÚ ešte nerozhodoval o podobných skutkových okolnostiach podľa GDPR, ktoré poskytuje viac usmernení k oblastiam, ktoré by sa mohli považovať za oblasti mimo rozsahu pôsobnosti právnych predpisov

209 Všeobecné nariadenie o ochrane údajov, odôvodnenie 18 a článok 2 ods. 2 písm. c); modernizovaný Dohovor č. 108, článok 3 ods. 2.

210 Všeobecné nariadenie o ochrane údajov, odôvodnenie 18.

211 Tamže, odôvodnenie 18, dôvodová správa k modernizovanému Dohovoru č. 108, ods. 29.

212 Pozri vyhlásenie pracovnej skupiny zriadenej podľa článku 29 o rokovaníach o balíku reforiem v oblasti ochrany údajov (2013), príloha 2: *Návrhy a zmeny týkajúce sa oslobodenia osobných alebo domácich činností*, 27. februára 2013.

213 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 28.

214 Pozri všeobecné nariadenie o ochrane údajov, odôvodnenie 18 a dôvodovú správu k modernizovanému Dohovoru č. 108, bod 27.

o ochrane údajov podľa „výnimky pre domácu činnosť“, ako je využívanie sociálnych médií na osobné účely.

Príklad: Vec *Bodil Lindquist*²¹⁵ sa týkala odkazovania na internetovej stránke na rôzne osoby prostredníctvom ich mena alebo iným spôsobom, napríklad na základe ich telefónneho čísla alebo informácií o ich záľubách. SDEÚ konštatoval, že: „operácia, ktorou sa odkazuje na internetovej stránke, na rôzne osoby a ktorou sa tieto osoby identifikujú buď prostredníctvom ich mena, alebo iným spôsobom [...] predstavuje „úplne alebo čiastočne automatizované spracúvanie osobných údajov“ v zmysle článku 3 ods. 1 smernice 95/46“²¹⁶.

Takéto spracúvanie osobných údajov nepredstavuje výlučne osobnú alebo domácu činnosť, ktorá je mimo rozsahu pôsobnosti pravidiel EÚ na ochranu údajov, keďže „táto výnimka sa musí vykladať tak, že sa vzťahuje výlučne na činnosti, ktoré patria do rámca súkromného alebo rodinného života jednotlivcov, čo zjavne neplatí v prípade spracovania osobných údajov, ktoré spočíva v ich zverejnení na internete takým spôsobom, že sa sprístupnia neobmedzenému počtu osôb“²¹⁷.

Podľa SDEÚ sa za určitých okolností môžu aj na obrazové záznamy súkromnej bezpečnostnej kamery vzťahovať právne predpisy EÚ o ochrane údajov.

Príklad: Vo veci *František Ryneš*²¹⁸ pán Ryneš domácim kamerovým systémom, ktorý nainštaloval na ochranu svojho majetku, zaznamenal obraz dvoch osôb, ktoré rozbili okná na jeho dome. Záznam bol následne odovzdaný polícii a bol použitý ako dôkaz počas trestného konania.

215 SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003.

216 Tamže, bod 27; predtým smernica 95/46, článok 3 ods. 1, teraz všeobecné nariadenie o ochrane údajov, článok 2 ods. 1.

217 SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003, bod 47.

218 SDEÚ, C-212/13, *František Ryneš/Úrad pro ochranu osobních údajů*, 11. decembra 2014, bod 33.

SDEÚ skonštatoval, že „[v] rozsahu, v akom taký kamerový systém [...] sníma, hoci len čiastočne, verejné priestranstvo, a smeruje mimo súkromnú sféru osoby, ktorá jeho prostredníctvom spracováva údaje, nemožno ho považovať za výlučne ‚osobnú či domácu‘ činnosť [...]“²¹⁹.

Prevádzkovateľ

V **právnych predpisoch EÚ** sa prevádzkovateľ vymedzuje ako niekoho, kto „sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov“²²⁰. Rozhodnutie prevádzkovateľa stanovuje, prečo a ako sa budú údaje spracúvať.

V **právnych predpisoch RE** sa v modernizovanom Dohovore č. 108 „prevádzkovateľ“ vymedzuje ako „fyzická alebo právnická osoba, orgán verejnej moci, útvar, agentúra alebo akýkoľvek iný subjekt, ktorý sám alebo spoločne s inými má rozhodovaciu právomoc v súvislosti so spracúvaním údajov“²²¹. Takáto rozhodovacia právomoc sa týka účelov a prostriedkov spracúvania, ako aj kategórií údajov, ktoré sa majú spracúvať, a prístupu k údajom²²². O tom, či táto právomoc vyplýva z právneho postavenia alebo zo skutkových okolností, sa musí rozhodnúť v jednotlivých prípadoch²²³.

Príklad: Vo veci *Google Spain*²²⁴ španielsky občan žiadal, aby Google odstránil starý novinový článok o jeho finančnej histórii.

SDEÚ bola položená otázka, či je spoločnosť Google ako poskytovateľ vyhľadávača „prevádzkovateľom“ údajov v zmysle článku 2 písm. d) smernice o ochrane údajov²²⁵. SDEÚ posudzoval širokú definíciu pojmu „prevádzko-

219 Predtým smernica 95/46, článok 3 ods. 2 druhá zarážka, teraz všeobecné nariadenie o ochrane údajov, článok 2 ods. 2 písm. c).

220 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 7.

221 Modernizovaný Dohovor č. 108, článok 2 písm. d).

222 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 22.

223 Tamže.

224 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014.

225 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 7; SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, bod 21.

vatel' na zaručenie „účinnnej a úplnej ochrany dotknutých osôb“²²⁶. SDEÚ konštatoval, že poskytovateľ vyhľadávača určoval účely a prostriedky činnosti a sprístupňoval údaje umiestnené na internetových stránkach editormi webových stránok každému používateľovi internetu, ktorý uskutočnil vyhľadávanie na základe mena dotknutej osoby²²⁷. SDEÚ preto dospel k záveru, že Google možno považovať za „prevádzkovateľa“²²⁸.

Ak prevádzkovateľ alebo sprostredkovateľ je usídlený mimo EÚ, spoločnosť musí písomne určiť zástupcu v rámci EÚ²²⁹. V GDPR sa zdôrazňuje, že zástupca musí byť usadený „v jednom z tých členských štátov, v ktorých sa nachádzajú dotknuté osoby, ktorých osobné údaje sa spracúvajú v súvislosti s ponukou tovaru alebo služieb pre nich, alebo ktorých správanie sa sleduje“²³⁰. Ak nie je určený žiadny zástupca, právne prostriedky môžu byť napriek tomu uplatnené proti samotnému prevádzkovateľovi alebo sprostredkovateľovi²³¹.

Spoločné prevádzkovateľstvo

V GDPR sa stanovuje, že ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi. To znamená, že spoločne rozhodujú o spracúvaní údajov na spoločný účel²³². V dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza, že v **rámci právnych predpisov RE** je možná aj existencia viacerých prevádzkovateľov alebo spoločných prevádzkovateľov²³³.

Pracovná skupina zriadená podľa článku 29 poukazuje na to, že spoločná kontrola môže mať rôzne podoby a že účasť rôznych prevádzkovateľov na kontrolných činnostiach nemusí byť rovnomerne rozdelená²³⁴. Takáto pružnosť umožňuje reagovať

226 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, bod 34.

227 Tamže, body 35 – 40.

228 Tamže, bod 41.

229 Všeobecné nariadenie o ochrane údajov, článok 27 ods. 1.

230 Tamže, článok 27 ods. 3.

231 Tamže, článok 27 ods. 5.

232 Tamže, článok 4 ods. 7 a článok 26.

233 Modernizovaný Dohovor č. 108, článok 2 písm. d); dôvodová správa k modernizovanému Dohovoru č. 108, ods. 22.

234 Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010, s. 19.

na rastúcu komplexnosť súčasnej situácie v oblasti spracúvania údajov²³⁵. Spoloční prevádzkovatelia musia preto určiť svoje príslušné oblasti zodpovednosti za plnenie povinností podľa tohto nariadenia na základe osobitnej dohody²³⁶.

Spoločné prevádzkovateľstvo vedie k spoločnej zodpovednosti za spracovateľskú činnosť²³⁷. V rámci **právnych predpisov** EÚ to znamená, že každý prevádzkovateľ alebo sprostredkovateľ môže niešť v plnej miere zodpovednosť za celú škodu spôsobenú spracúvaním v rámci spoločnej kontroly, aby sa dotknutej osobe zabezpečila účinná náhrada²³⁸.

Príklad: Bežným príkladom spoločného prevádzkovateľstva je databáza dlžníkov vedená spoločne niekoľkými úverovými inštitúciami. Ak niekto požiada o úver v banke, ktorá je jedným zo spoločných prevádzkovateľov, banky nahliadnu do databázy, ktorá im pomôže prijať informované rozhodnutie o úverovej bonite žiadateľa.

V právnych predpisoch sa výslovne nestanovuje, či sa pri spoločnom prevádzkovateľstve vyžaduje, aby všetci prevádzkovatelia mali rovnaký spoločný účel, alebo či stačí, ak sa ich účely len čiastočne prekrývajú. Zatiaľ nie je k dispozícii žiadna relevantná judikatúra na európskej úrovni. Pracovná skupina zriadená podľa článku 29 vo svojom stanovisku z roku 2010 o prevádzkovateľoch a spracovateľoch (sprostredkovateľoch) uvádza, že spoloční prevádzkovatelia môžu mať spoločné všetky účely a prostriedky spracúvania alebo sa môžu podieľať len na niektorých účeloch alebo prostriedkoch, alebo ich častiach²³⁹. Zatiaľ čo prvá možnosť by znamenala veľmi úzky vzťah medzi rôznymi aktérmi, druhá možnosť by naznačovala voľnejší vzťah.

Pracovná skupina zriadená podľa článku 29 obhajuje široký výklad pojmu spoloční prevádzkovatelia s cieľom umožniť určitú flexibilitu pri reagovaní na stále komplexnejšiu situáciu v oblasti spracúvania údajov²⁴⁰. Túto pozíciu pracovnej skupiny ilustruje prípad týkajúci sa Spoločnosti pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT).

235 Tamže.

236 Všeobecné nariadenie o ochrane údajov, odôvodnenie 79.

237 Tamže, bod 21.

238 Tamže, článok 82 ods. 4.

239 Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010, s. 19.

240 Tamže.

Príklad: V tzv. prípade SWIFT európske bankové inštitúcie využívali spoločnosť SWIFT, spočiatku ako sprostredkovateľa, pri realizácii prenosu osobných údajov v rámci bankových transakcií. Spoločnosť SWIFT sprístupnila údaje o bankových transakciách uložené v počítačovom servisnom stredisku v Spojených štátoch amerických Ministerstvu financií USA bez toho, aby jej to výslovne nariadili európske bankové inštitúcie, ktoré využívali jej služby. Pracovná skupina zriadená podľa článku 29 dospela pri hodnotení zákonnosti tohto postupu k záveru, že európske bankové inštitúcie využívajúce spoločnosť SWIFT, ako aj spoločnosť SWIFT ako takú, treba považovať za spoločných prevádzkovateľov zodpovedných voči európskym zákazníkom za poskytnutie ich údajov americkým orgánom²⁴¹.

Sprostredkovateľ

Sprostredkovateľ je **podľa práva EÚ** vymedzený ako osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa²⁴². Činnosti, ktorými je sprostredkovateľ poverený, môžu byť obmedzené na veľmi špecifickú úlohu alebo kontext alebo môžu byť pomerne všeobecné a komplexné.

Podľa právnych predpisov RE je význam pojmu sprostredkovateľ rovnaký ako podľa právnych predpisov EÚ²⁴³.

Okrem spracúvania údajov pre iných budú sprostredkovatelia aj prevádzkovateľmi vo vzťahu k spracúvaniu, ktoré vykonávajú na vlastné účely, napríklad na účely riadenia svojich vlastných zamestnancov, predaja a účtovníctva.

Príklad: Spoločnosť Everready sa špecializuje na spracúvanie údajov pri riadení údajov o ľudských zdrojoch pre iné spoločnosti. V tejto funkcii je spoločnosť Everready sprostredkovateľom. Ak však spoločnosť Everready spracúva údaje o svojich vlastných zamestnancoch, je prevádzkovateľom pri spracovateľských operáciách na účely plnenia svojich povinností ako zamestnávateľa.

241 Pracovná skupina zriadená podľa článku 29 (2006), *Stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT)*, WP 128, Brusel, 22. novembra 2006.

242 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 8.

243 Modernizovaný Dohovor č. 108, článok 2 písm. f).

Vzťah medzi prevádzkovateľom a sprostredkovateľom

Ako už bolo uvedené, prevádzkovateľ je vymedzený ako subjekt, ktorý určuje účely a prostriedky spracúvania. V GDPR sa jasne uvádza, že sprostredkovateľ môže spracúvať osobné údaje len na základe pokynov prevádzkovateľa, s výnimkou prípadov, keď sa to vyžaduje podľa práva Únie alebo práva členského štátu²⁴⁴. Zmluva medzi prevádzkovateľom a sprostredkovateľom je základným prvkom ich vzťahu a je právnou požiadavkou²⁴⁵.

Príklad: Riaditeľ spoločnosti Sunshine sa rozhodne, že spoločnosť Cloudy Company s odborným zameraním na cloudové úložiská má spravovať údaje o zákazníkoch spoločnosti Sunshine. Spoločnosť Sunshine Company je aj naďalej prevádzkovateľom a spoločnosť Cloudy Company je len sprostredkovateľom, keďže v súlade so zmluvou môže spoločnosť Cloudy použiť údaje o zákazníkoch spoločnosti Sunshine len na účely, ktoré určí spoločnosť Sunshine.

Ak je právomoc určiť prostriedky spracúvania delegovaná na sprostredkovateľa, prevádzkovateľ musí byť napriek tomu schopný vykonávať primeraný stupeň kontroly nad rozhodnutiami sprostredkovateľa, pokiaľ ide o prostriedky spracúvania. Celkovú zodpovednosť stále nesie prevádzkovateľ, ktorý musí vykonávať dohľad nad sprostredkovateľmi s cieľom zabezpečiť, aby ich rozhodnutia boli v súlade s právnymi predpismi o ochrane údajov a s jeho vlastnými pokynmi.

Okrem toho, ak sprostredkovateľ nedodrížiava podmienky spracúvania údajov stanovené prevádzkovateľom, sprostredkovateľ sa stane prevádzkovateľom minimálne v rozsahu porušenia pokynov prevádzkovateľa. S najväčšou pravdepodobnosťou sa takto zo sprostredkovateľa stane prevádzkovateľ, ktorý koná protiprávne. Pôvodný prevádzkovateľ naopak musí vysvetliť, ako sprostredkovateľ mohol porušiť jeho pokyny²⁴⁶. Pracovná skupina zriadená podľa článku 29 v takýchto prípadoch zvykne predpokladať existenciu spoločných prevádzkovateľov, keďže to vedie k najlepšej ochrane záujmov dotknutých osôb²⁴⁷.

244 Všeobecné nariadenie o ochrane údajov, článok 29.

245 Tamže, článok 28 ods. 3.

246 Tamže, článok 82 ods. 2.

247 Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010, s. 25; Pracovná skupina zriadená podľa článku 29 (2006), *Stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT)*, WP 128, Brusel, 22. novembra 2006.

Rozdelenie zodpovednosti môže byť problematické aj v prípade, že prevádzkovateľom je malý podnik a sprostredkovateľom veľká obchodná spoločnosť, ktorá môže diktovať podmienky poskytovania svojich služieb. Za týchto okolností však pracovná skupina zriadená podľa článku 29 tvrdí, že úroveň zodpovednosti by sa nemala znižovať z dôvodu hospodárskej nerovnováhy a že sa musí zachovať chápanie pojmu prevádzkovateľ²⁴⁸.

V záujme jasnosti a transparentnosti sa podrobnosti vzťahu medzi prevádzkovateľom a sprostredkovateľom musia zaznamenať v písomnej zmluve²⁴⁹. Zmluva musí obsahovať najmä predmet, povahu, účel a trvanie spracúvania, druh osobných údajov a kategórie dotknutých osôb. Takisto by sa v nej mali stanoviť povinnosti a práva prevádzkovateľa a sprostredkovateľa, ako sú požiadavky týkajúce sa dôverylosti a bezpečnosti. Bez takejto zmluvy prevádzkovateľ porušuje svoju povinnosť písomne dokumentovať vzájomné povinnosti, čo môže viesť k sankciám. Ak v dôsledku konania nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade s právom, vznikla škoda, zodpovednosť nenesie len prevádzkovateľ, ale aj sprostredkovateľ²⁵⁰. Sprostredkovateľ musí viesť záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonáva v mene prevádzkovateľa²⁵¹. Tieto záznamy sa na požiadanie sprístupnia dozornému orgánu, keďže prevádzkovateľ a sprostredkovateľ musia pri plnení svojich úloh spolupracovať s týmto orgánom²⁵². Prevádzkovatelia a sprostredkovatelia takisto majú možnosť pristúpiť k schválenému kódexu správania alebo certifikačnému mechanizmu na preukázanie svojho súladu s požiadavkami GDPR²⁵³.

Sprostredkovateľ môže mať záujem poveriť určitými úlohami ďalších sprostredkovateľov. Je to právne prípustné, ak si prevádzkovateľ a sprostredkovateľ medzi sebou dohodnú vhodné zmluvné ustanovenia vrátane toho, či je v každom jednotlivom prípade potrebné povolenie prevádzkovateľa alebo či postačuje iba oznámenie. V GDPR sa stanovuje, že ak tento ďalší sprostredkovateľ nesplní svoje povinnosti ochrany údajov, pôvodný sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný²⁵⁴.

248 Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010, s. 26.

249 Všeobecné nariadenie o ochrane údajov, článok 28 ods. 3 a ods. 9.

250 Tamže, článok 82 ods. 2.

251 Tamže, článok 30 ods. 2.

252 Tamže, článok 30 ods. 4 a článok 31.

253 Tamže, článok 28 ods. 5 a článok 42 ods. 4.

254 Tamže, článok 28 ods. 4.

Právne predpisy RE v plnej miere uplatňujú výklad pojmov prevádzkovateľ a sprostredkovateľ tak, ako sú vysvetlené vyššie²⁵⁵.

2.3.2. Prijemcovia a tretie strany

Rozdiel medzi týmito dvomi kategóriami osôb alebo subjektov, ktoré boli zavedené v smernici o ochrane údajov, spočíva predovšetkým v ich vzťahu k prevádzkovateľovi a následne v ich povolení na prístup k osobným údajom uchovávaných prevádzkovateľom.

„Tretia strana“ je subjekt, ktorý sa líši od prevádzkovateľa a sprostredkovateľa. Podľa článku 4 bodu 10 GDPR tretia strana „je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov“. Znamená to, že osoby pracujúce pre inú organizáciu než je prevádzkovateľ – aj keď patrí do tej istej skupiny alebo holdingovej spoločnosti – sa budú považovať (alebo sa považujú) za „tretie strany“. Na druhej strane, pobočky banky, ktoré pracujú s účtami klienta na základe priameho poverenia ich ústredia, sa nepovažujú za „tretie strany“²⁵⁶.

„Prijemca“ je širší pojem než „tretia strana“. V zmysle článku 4 bodu 9 GDPR príjemca znamená „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou“. Prijemcom môže byť osoba mimo prevádzkovateľa alebo sprostredkovateľa (tá by potom bola treťou stranou) alebo niekto, kto pôsobí v rámci prevádzkovateľa alebo sprostredkovateľa, napríklad zamestnanec inej divízie v rámci rovnakej spoločnosti alebo orgánu.

Rozdiel medzi príjemcami a tretími stranami je dôležitý nielen z hľadiska podmienok zákonného poskytovania údajov. Zamestnanci prevádzkovateľa alebo sprostredkovateľa môžu byť príjemcami osobných údajov bez ďalších právnych požiadaviek, ak sú zapojení do spracovateľských operácií prevádzkovateľa alebo sprostredkovateľa. Keďže tretia strana je od prevádzkovateľa alebo sprostredkovateľa nezávislá, nie je oprávnená používať osobné údaje, ktoré prevádzkovateľ spracúva, pokiaľ v konkrétnom prípade neexistujú osobitné právne dôvody.

²⁵⁵ Pozri napríklad modernizovaný Dohovor č. 108, článok 2 písm. b) a f); odporúčanie o profilovaní, článok 1.

²⁵⁶ Pracovná skupina zriadená podľa článku 29 (2010), *Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“*, WP 169, Brusel, 16. februára 2010, s. 31.

Príklad: Zamestnanec prevádzkovateľa, ktorý používa osobné údaje pri plnení úloh, ktorými ho zamestnávateľ poveril, je príjemcom údajov, nie je však treťou stranou, keďže používa údaje v mene prevádzkovateľa a podľa jeho pokynov. Napríklad, ak zamestnávateľ poskytuje osobné údaje o svojich zamestnancoch svojmu oddeleniu ľudských zdrojov z dôvodu nadchádzajúcich hodnotení pracovného výkonu, oddelenie ľudských zdrojov bude príjemcom osobných údajov, keďže údaje mu boli poskytnuté v priebehu spracúvania pre prevádzkovateľa.

Ak však organizácia poskytne údaje o svojich zamestnancoch vzdelávacej spoločnosti, ktorá ich použije na prispôbenie programu odbornej prípravy pre zamestnancov, táto spoločnosť je treťou stranou. Je to preto, že vzdelávacia spoločnosť nemá konkrétne oprávnenie ani povolenie (v prípade „oddelenia ľudských zdrojov“ vyplýva z pracovnoprávneho vzťahu s prevádzkovateľom) na spracúvanie týchto osobných údajov. Inými slovami, informácie jej neboli poskytnuté v rámci pracovnoprávneho vzťahu s prevádzkovateľom.

2.4. Súhlas

Hlavné body

- Súhlas ako právny základ na spracúvanie osobných údajov musí byť slobodne daný, informovaný, konkrétny a jednoznačný prejav vôle s jednoznačným potvrdzujúcim úkonom vyjadrujúcim súhlas so spracúvaním.
- Spracúvanie osobitných kategórií údajov si vyžaduje výslovný súhlas.

Ako sa podrobne uvádza v kapitole 4, súhlas je jedným zo šiestich legitímnych dôvodov na spracúvanie osobných údajov. Súhlas znamená „akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby“²⁵⁷.

²⁵⁷ Všeobecné nariadenie o ochrane údajov, článok 4 ods. 11. Pozri aj modernizovaný Dohovor č. 108, článok 5 ods. 2.

V **právnych predpisoch EÚ** sa stanovuje niekoľko prvkov, ktoré sú potrebné, aby bol súhlas platný, pričom ich cieľom je zaručiť, aby dotknuté osoby skutočne súhlasili s konkrétnym využitím svojich údajov²⁵⁸.

- Súhlas sa musí poskytnúť jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním jej osobných údajov. Takýmto prejavom môže byť konanie alebo vyhlásenie.
- Dotknutá osoba musí mať právo kedykoľvek odvolať svoj súhlas.
- V rámci písomného vyhlásenia, ktoré sa vzťahuje aj na iné veci, ako sú „podmienky poskytovania služieb“, musí byť žiadosť o súhlas uvedená jasne a jednoducho, a v zrozumiteľnej a ľahko dostupnej forme, pričom sa jasne odlišuje súhlas od iných záležitostí; ak nejaká časť takéhoto vyhlásenia porušuje GDPR, nie je záväzná.

Súhlas bude v kontexte právnych predpisov o ochrane údajov platný len v prípade, že sú splnené všetky tieto požiadavky. Je povinnosťou prevádzkovateľa preukázať, že dotknutá osoba súhlasila so spracúvaním svojich údajov²⁵⁹. Prvky platného súhlasu sú podrobnejšie opísané v **oddiele 4.1.1** o právnych základoch na spracúvanie osobných údajov.

Dohovor č. 108 neobsahuje definíciu pojmu súhlas; jeho vymedzenie sa ponecháva na právne predpisy jednotlivých štátov. V **právnych predpisoch RE** prvky platného súhlasu zodpovedajú prvkom, ktoré tu už boli opísané²⁶⁰.

Dodatočné požiadavky na platný súhlas podľa občianskeho práva, napríklad právna spôsobilosť, sa prirodzene uplatňujú aj v súvislosti s ochranou údajov, keďže takéto požiadavky sú základnými právnymi predpokladmi. Neplatný súhlas osôb, ktoré nemajú právnu spôsobilosť, povedie k tomu, že bude chýbať právny základ na spracúvanie údajov o takýchto osobách. Pokiaľ ide o právnu spôsobilosť maloletých osôb uzatvárať zmluvy, v GDPR sa stanovuje, že jeho pravidlá týkajúce

²⁵⁸ Všeobecné nariadenie o ochrane údajov, článok 7.

²⁵⁹ Tamže, článok 7 ods. 1.

²⁶⁰ Modernizovaný Dohovor č. 108, článok 5 ods. 2; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42 – 45.

sa minimálneho veku na získanie platného súhlasu nemajú vplyv na všeobecné zmluvné právo členských štátov²⁶¹.

Súhlas sa musí poskytnúť jednoznačným spôsobom, aby nevznikli pochybnosti o úmysle dotknutej osoby²⁶². Súhlas musí byť výslovný, ak sa týka spracúvania citlivých údajov, a môže sa poskytnúť ústne alebo písomne²⁶³. Písomne sa môže poskytnúť aj elektronickými prostriedkami²⁶⁴. V rámci **právnych predpisov EÚ a RE** sa musí súhlas so spracúvaním osobných údajov poskytnúť vo forme vyhlásenia alebo prostredníctvom jednoznačného potvrdzujúceho úkonu²⁶⁵. Súhlas preto nemožno vyvodiť z mlčania, vopred označených políček alebo nečinnosti²⁶⁶.

261 Všeobecné nariadenie o ochrane údajov, článok 8 ods. 3.

262 Tamže, článok 6 ods. 1 písm. a) a článok 9 ods. 2 písm. a).

263 Tamže, odôvodnenie 32.

264 Tamže.

265 Tamže, článok 4 ods. 11, dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42.

266 Všeobecné nariadenie o ochrane údajov, odôvodnenie 32; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42.

3

Hlavné zásady európskeho práva v oblasti ochrany údajov

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a)	Zásada zákonnosti	Modernizovaný Dohovor č. 108, článok 5 ods. 3
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a)	Zásada spravodlivosti	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. a) ESLP, <i>K.H. a i./Slovensko</i> , č. 32881/04, 2009
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a) SDEÚ, C-201/14, <i>Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.</i> , 2015	Zásada transparentnosti	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. a) a článok 8 ESLP, <i>Haralambie/Rumunsko</i> , č. 21737/03, 2009
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. b)	Zásada obmedzenia účelu	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b)
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. c) SDEÚ, spojené veci C-293/12 a C-594/12, <i>Digital Rights Ireland a Kärntner Landesregierung a i. [VK]</i> , 2014	Zásada minimalizácie údajov	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. c)
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. d) SDEÚ, C-553/07, <i>College van burgemeester en wethouders van Rotterdam/M. E. Rijkeboer</i> , 2009	Zásada správnosti údajov	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. d)

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. e) SDEÚ, spojené veci C-293/12 a C-594/12, <i>Digital Rights Ireland a Kärntner Landesregierung a i. [VK]</i> , 2014	Zásada minimalizácie uchovávania	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. e) ESLP, <i>S. a Marper/Spojené kráľovstvo [VK]</i> , č. 30562/04 a č. 3056/04, 2008
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. f) a článok 32	Zásada bezpečnosti (integrity a dôverylosti) údajov	Modernizovaný Dohovor č. 108, článok 7
Všeobecné nariadenie o ochrane údajov, článok 5 ods. 2	Zásada zodpovednosti	Modernizovaný Dohovor č. 108, článok 10

V článku 5 všeobecného nariadenia o ochrane údajov sa stanovujú zásady spracúvania osobných údajov. Tieto zásady zahŕňajú:

- zákonnosť, spravodlivosť a transparentnosť,
- obmedzenie účelu,
- minimalizáciu údajov,
- správnosť údajov,
- minimalizáciu uchovávania,
- integritu a dôverynosť.

Tieto zásady slúžia ako východisko pre podrobnejšie ustanovenia v nasledujúcich článkoch nariadenia. Nachádzajú sa aj v článkoch 5, 7, 8 a 10 modernizovaného Dohovoru č. 108. Všetky novšie právne predpisy v oblasti ochrany údajov na úrovni RE alebo EÚ musia byť v súlade s týmito zásadami a pri výklade týchto právnych predpisov sa tieto zásady musia zohľadňovať. Podľa právnych predpisov EÚ sú obmedzenia týkajúce sa zásad spracúvania povolené len v rozsahu, v akom zodpovedajú právam a povinnostiam stanoveným v článkoch 12 až 22, a musia rešpektovať podstatu základných práv a slobôd. Výnimky a obmedzenia týchto základných zásad sa môžu stanoviť na úrovni EÚ alebo na vnútroštátnej úrovni²⁶⁷; musia byť stanovené zákonom, sledovať legitímny cieľ a predstavovať nevyhnutné a primerané opatrenia v demokratickej spoločnosti²⁶⁸. Všetky tri podmienky musia byť splnené.

²⁶⁷ Modernizovaný Dohovor č. 108, článok 11 ods. 1, všeobecné nariadenie o ochrane údajov, článok 23 ods. 1.

²⁶⁸ Všeobecné nariadenie o ochrane údajov, článok 23 ods. 1.

3.1. Zásady zákonnosti, spravodlivosti a transparentnosti spracúvania

Hlavné body

- Zásady zákonnosti, spravodlivosti a transparentnosti sa vzťahujú na spracúvanie všetkých osobných údajov.
- Podľa GDPR sa na účely zákonnosti požaduje:
 - súhlas dotknutej osoby,
 - nevyhnutnosť uzatvorenia zmluvy,
 - zákonná povinnosť,
 - nevyhnutnosť ochrany životne dôležitých záujmov dotknutej osoby alebo inej osoby,
 - nevyhnutnosť splnenia úlohy vo verejnom záujme,
 - nevyhnutnosť oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo práva a slobody dotknutej osoby.
- Spracúvanie osobných údajov by sa malo vykonávať spravodlivo.
 - Dotknutá osoba musí byť informovaná o riziku, aby sa zabezpečilo, že spracúvanie nebude mať nepredvídateľné negatívne účinky.
- Spracúvanie osobných údajov by sa malo vykonávať transparentne.
 - Prevádzkovatelia musia informovať dotknuté osoby pred spracúvaním ich údajov, okrem iného aj o účele spracúvania a totožnosti a adrese prevádzkovateľa.
 - Informácie o spracovateľských operáciách musia byť formulované jasne a jednoducho, aby dotknuté osoby dokázali ľahko pochopiť pravidlá, riziká, záruky a práva súvisiace so spracúvaním.
 - Dotknuté osoby majú právo na prístup k svojim údajom bez ohľadu na to, kde sa spracúvajú.

3.1.1. Zákonnosť spracúvania

Podľa **právnych predpisov EÚ a RE** o ochrane údajov sa vyžaduje, aby sa osobné údaje spracúvali zákonným spôsobom²⁶⁹. Zákonné spracúvanie si vyžaduje súhlas dotknutej osoby alebo iný legitímny dôvod podľa právnych predpisov o ochrane údajov²⁷⁰. V článku 6 ods. 1 GDPR sa okrem súhlasu uvádza päť právnych základov spracúvania, t. j. ak je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, plnenie úlohy realizovanej pri výkone verejnej moci, splnenie zákonnej povinnosti, na účely oprávnených záujmov prevádzkovateľa alebo tretích strán alebo ak je to potrebné na ochranu životne dôležitých záujmov dotknutej osoby. Podrobnejšie informácie sú uvedené v [oddiele 4.1](#).

3.1.2. Spravodlivosť spracúvania

Okrem zákonného spracúvania sa v právnych predpisoch EÚ a RE o ochrane údajov vyžaduje, aby sa osobné údaje spracúvali spravodlivo²⁷¹. Zásada spravodlivého spracúvania v prvom rade upravuje vzťah medzi prevádzkovateľom a dotknutou osobou.

Prevádzkovatelia by mali oznámiť dotknutým osobám a širokej verejnosti, že spracujú údaje zákonným a transparentným spôsobom, a musia byť schopní preukázať súlad spracovateľských operácií s GDPR. Spracovateľské operácie sa nesmú vykonávať v tajnosti a dotknuté osoby by mali byť informované o potenciálnych rizikách. Okrem toho, pokiaľ je to možné, prevádzkovatelia musia čo najrýchlejšie reagovať na požiadavky dotknutej osoby, najmä ak jej súhlas tvorí právny základ na spracúvanie údajov.

Príklad: Vo veci *K. H. a iní/Slovensko* ²⁷² boli sťažovateľky – ženy rómskeho pôvodu – počas tehotenstva a pri pôrode ošetrované v dvoch nemocniciach na východnom Slovensku. Po tomto ošetrení ani jedna z nich nemohla počať ďalšie dieťa, a to napriek opakovaným pokusom. Vnútroštátne súdy nariadili

269 Modernizovaný Dohovor č. 108, článok 5 ods. 3, všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a).

270 Charta základných práv Európskej únie, článok 8 ods. 2; všeobecné nariadenie o ochrane údajov, odôvodnenie 40 a články 6 – 9; modernizovaný Dohovor č. 108, článok 5 ods. 2; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 41.

271 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. a).

272 *ESLP, K.H. a i./Slovensko*, č. 32881/04, 28. apríla 2009.

nemocniciam, aby povolili sťažovateľkám a ich zástupcom nahliadnuť do lekárskeho záznamu a urobiť písomné výňatky z nich, ale zamietli ich žiadosť o vytvorenie fotokópií dokumentov, údajne preto, aby zabránili ich zneužitiu. Pozitívne povinnosti štátu vyplývajúce z článku 8 ECHR zahŕňajú povinnosť sprístupniť dotknutej osobe kópie spisov s jej údajmi. Štát bol povinný určiť podmienky kopírovania spisov s osobnými údajmi alebo (podľa okolností) uviesť presvedčivé dôvody zamietnutia ich kopírovania. V prípade sťažovateľiek vnútroštátne súdy zdôvodnili zákaz vyhotovenia fotokópií lekárskeho záznamu v podstate potrebou chrániť relevantné informácie pred zneužitím. ESĽP si však nedokázal predstaviť, akým spôsobom by sťažovateľky, ktorým aj tak bol umožnený prístup k celému lekárskeму spisu, mohli zneužiť informácie, ktoré sa ich týkajú. Okrem toho, riziku zneužitia bolo možné predísť iným spôsobom ako zamietnutím kopírovania spisov, napríklad obmedzením počtu osôb, ktoré majú k spisom prístup. Štát nepreukázal existenciu dostatočne presvedčivých dôvodov na zamietnutie efektívneho prístupu sťažovateľiek k informáciám, ktoré sa týkajú ich zdravia. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

V súvislosti s internetovými službami musia vlastnosti systémov, ktoré spracúvajú osobné údaje, dotknutým osobám umožniť skutočne pochopiť, čo sa deje s ich údajmi. Zásada spravodlivosti v každom prípade presahuje rámec povinností týkajúcich sa transparentnosti a môže súvisieť aj s etickým spôsobom spracúvania osobných údajov.

Príklad: Výskumné oddelenie univerzity vykonáva pokus, pri ktorom analyzuje zmeny nálad 50 účastníkov. Tí musia v elektronickom súbore každú hodinu v určitom čase evidovať svoje myšlienky. Týchto 50 osôb vyjadrilo súhlas s týmto konkrétnym projektom a s týmto konkrétnym použitím údajov zo strany univerzity. Výskumné oddelenie čoskoro zistí, že elektronické zaznamenávanie myšlienok by bolo veľmi užitočné pri inom projekte zameranom na duševné zdravie, ktorého koordináciu má na starosti iný tím. Aj keď univerzita ako prevádzkovateľ mohla použiť tie isté údaje pri práci iného tímu bez ďalších krokov na zabezpečenie zákonnosti spracúvania týchto údajov, keďže tieto účely sú zlučiteľné, univerzita v súlade so svojim etickým kódexom v oblasti výskumu a zásadou spravodlivého spracúvania informovala účastníkov a požiadala ich o nový súhlas.

3.1.3. Transparentnosť spracúvania

Podľa **právnych predpisov** EÚ a RE o ochrane údajov sa vyžaduje, aby sa spracúvanie osobných údajov vykonávalo „transparentne vo vzťahu k dotknutej osobe“²⁷³.

Touto zásadou sa stanovuje povinnosť prevádzkovateľa prijať akékoľvek vhodné opatrenie s cieľom informovať dotknuté osoby – ktoré môžu byť používateľmi, zákazníkmi alebo klientmi – o tom, ako sa ich údaje používajú²⁷⁴. Transparentnosť sa môže vzťahovať na informácie poskytnuté osobám pred začatím spracúvania²⁷⁵, informácie, ktoré by mali byť ľahko dostupné dotknutým osobám počas spracúvania²⁷⁶, ale aj na informácie poskytnuté dotknutým osobám na základe žiadosti o prístup k ich vlastným údajom²⁷⁷.

Príklad: Sťažovateľovi vo veci *Haralambie/Rumunsko*²⁷⁸ bol umožnený prístup k informáciám, ktoré o ňom uchovávala tajná služba, až o päť rokov po tom, čo o tento prístup požiadal. ESĽP pripomenul, že jednotlivci, o ktorých verejné orgány vedú osobné spisy, majú životne dôležitý záujem na sprístupnení týchto spisov. Orgány sú povinné zaistiť efektívny spôsob získania prístupu k takýmto informáciám. ESĽP sa domnieval, že ani množstvo poskytnutých spisov, ani nedostatky v systéme archivácie neodôvodňujú päťročné zdržanie pri vybavovaní žiadosti sťažovateľa a povolení prístupu k jeho spisom. Orgány nezabezpečili efektívny a dostupný postup, ktorým by sa sťažovateľovi umožnilo získať prístup k jeho osobným spisom v primeranom čase. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Spracovateľské operácie musia byť dotknutým osobám vysvetlené ľahko prístupným spôsobom, ktorým sa zaručí, že dotknuté osoby chápu, čo sa bude diať s ich údajmi. To znamená, že konkrétny účel spracúvania osobných údajov musí byť dotknutej osobe známy v čase získavania osobných údajov²⁷⁹. Transparentnosť spracúvania si

273 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. a); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. a) a článok 8.

274 Všeobecné nariadenie o ochrane údajov, článok 12.

275 Tamže, článok 13 a 14.

276 Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 2/2017 k spracúvaniu údajov v práci*, s. 23.

277 Všeobecné nariadenie o ochrane údajov, článok 15.

278 ESĽP, *Haralambie/Rumunsko*, č. 21737/03, 27. októbra 2009.

279 Všeobecné nariadenie o ochrane údajov, odôvodnenie 39.

vyžaduje, aby sa používal jasný a jednoduchý jazyk²⁸⁰. Dotknutým osobám musí byť jasné, aké sú riziká, pravidlá, záruky a práva týkajúce sa spracúvania ich osobných údajov²⁸¹.

Právne predpisy RE takisto uvádzajú, že určité základné informácie prevádzkovateľ musí povinne iniciatívne poskytovať dotknutým osobám. Informácie o názve a adrese prevádzkovateľa (alebo spoločných prevádzkovateľov), právnom základe a účeloch spracúvania údajov, kategóriách spracúvaných údajov a príjemcoch, ako aj spôsobe uplatňovania práv sa môžu poskytovať v akejkoľvek vhodnom formáte (buď prostredníctvom webového sídla, technologických nástrojov na osobných zariadeniach atď.), pokiaľ sú tieto informácie dotknutej osobe poskytnuté náležite a účinne. Poskytnuté informácie by mali byť ľahko dostupné, čitateľné, zrozumiteľné a prispôbené príslušným dotknutým osobám (napríklad v jazyku primeranom pre deti). Poskytnú sa aj akékoľvek dodatočné informácie, ktoré sú potrebné na zabezpečenie spravodlivého spracúvania údajov alebo ktoré sú užitočné na takýto účel, napríklad obdobie uchovávanía údajov, informácie o dôvodoch spracúvania údajov alebo informácie o prenose údajov príjemcovi u inej strany alebo tretej strane (vrátane informácií o tom, či táto konkrétna tretia strana poskytuje primeranú úroveň ochrany alebo o opatreniach, ktoré prevádzkovateľ prijal na zaručenie takejto primeranej úrovne ochrany údajov)²⁸².

Na základe práva na prístup²⁸³ má dotknutá osoba právo na to, aby ju prevádzkovateľ na požiadanie informoval, či sa jej údaje spracúvajú, a ak áno, ktoré údaje sa spracúvajú²⁸⁴. Okrem toho, podľa práva na informácie²⁸⁵ musia prevádzkovatelia alebo sprostredkovatelia v zásade pred začatím spracovateľských činností iniciatívne informovať osoby, ktorých údaje spracúvajú, o účeloch, trvaní, prostriedkoch spracúvania a iných podrobnostiach.

280 Tamže.

281 Tamže.

282 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 68.

283 Všeobecné nariadenie o ochrane údajov, článok 15.

284 Modernizovaný Dohovor č. 108, článok 8 a článok 9 ods. 1 písm. b).

285 Všeobecné nariadenie o ochrane údajov, článok 13 a 14.

Príklad: *Vec Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*²⁸⁶ sa týkala poskytnutia daňových údajov týkajúcich sa príjmov samostatne zárobkovo činných osôb z Národnej agentúry pre daňovú správu do Národnej zdravotnej poisťovne v Rumunsku, pričom na základe týchto údajov sa požadovalo zaplatenie nedoplatkov na príspevkoch na zdravotné poistenie. SDEÚ bol požiadaný, aby určil, či dotknutá osoba mala byť predbežne informovaná o totožnosti prevádzkovateľa a účele poskytnutia údajov pred tým, ako tieto údaje spracúvala Národná zdravotná poisťovňa. SDEÚ rozhodol, že ak verejná inštitúcia členského štátu zasiela osobné údaje inej verejnej inštitúcii, ktorá tieto údaje ďalej spracúva, dotknuté osoby musia byť informované o tomto poskytnutí alebo spracúvaní.

V určitých situáciách sú povolené výnimky z povinnosti informovať dotknuté osoby o spracúvaní údajov, sú podrobnejšie uvedené v [oddiele 6.1](#) o právach dotknutej osoby.

3.2. Zásada obmedzenia účelu

Hlavné body

- Účel spracúvania údajov sa musí definovať pred začatím spracúvania.
- Ďalšie spracúvanie údajov nemôže byť nezlučiteľné s pôvodným účelom, hoci vo všeobecnom nariadení o ochrane údajov sa stanovujú výnimky z tohto pravidla na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu a na štatistické účely.
- Zásada obmedzenia účelu v podstate znamená, že každé spracúvanie osobných údajov sa musí vykonávať na konkrétne vymedzené účely a len na dodatočné, konkrétne účely, ktoré sú zlučiteľné s pôvodným účelom.

Zásada obmedzenia účelu je jednou zo základných zásad európskych právnych predpisov v oblasti ochrany údajov. Úzko sa spája s transparentnosťou, predvídateľnosťou a kontrolou používateľa: ak je účel spracúvania dostatočne konkrétny a jasný, jednotlivci vedia, čo možno očakávať, čím sa posilňuje transparentnosť a právna

²⁸⁶ SDEÚ, C-201/14, *Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*, 1. októbra 2015, body 28 – 46.

istota. Zároveň je dôležité jasné vymedzenie účelu, aby dotknuté osoby mohli účinne uplatňovať svoje práva, napríklad právo namietat proti spracúvaniu²⁸⁷.

Táto zásada si vyžaduje, aby sa každé spracúvanie osobných údajov vykonávalo na konkrétny, dobre vymedzený účel a len na dodatočné účely, ktoré sú zlučiteľné s pôvodným účelom²⁸⁸. Spracúvanie osobných údajov na neurčité a/alebo neobmedzené účely je teda nezákonné. Spracúvanie osobných údajov bez určitého účelu, ktoré je založené len na tom, že by mohli byť užitočné niekedy v budúcnosti, nie je zákonné. Legitímnosť spracúvania osobných údajov bude závisieť od účelu spracúvania, ktorý musí byť výslovne uvedený, konkrétny a legitímny.

Každý nový účel spracúvania údajov, ktorý nie je zlučiteľný s pôvodným účelom, musí mať svoj vlastný právny základ a nemôže sa odvolávať na skutočnosť, že údaje boli pôvodne získané alebo spracúvané na iný legitímny účel. Na druhej strane je legitímne spracúvanie obmedzené na spracúvanie na pôvodný uvedený účel a každý nový účel spracúvania si bude vyžadovať samostatný nový právny základ. Napríklad poskytnutie osobných údajov tretím stranám na nový účel sa bude musieť starostlivo zvážiť, keďže takéto poskytnutie si pravdepodobne bude vyžadovať dodatočný právny základ, odlišný od právneho základu, na základe ktorého sa tieto údaje získali.

Príklad: Letecká spoločnosť zbiera údaje svojich cestujúcich pri rezerváciách, aby mohla riadne prevádzkovať lety. Bude potrebovať údaje o: číslach sedadiel cestujúcich, osobitných fyzických obmedzeniach, napríklad u osôb na invalidnom vozíku, a v súvislosti s osobitnými požiadavkami na stravu (napríklad kóšer alebo halal). Ak letecké spoločnosti musia poskytnúť tieto údaje uvedené v zázname o cestujúcom imigračným orgánom na prístávacom letisku, údaje sú následne použité na účely imigračnej kontroly, teda účely, ktoré sa odlišujú od pôvodného účelu získania údajov. Poskytnutie uvedených údajov imigračným orgánom si bude teda vyžadovať nový a samostatný právny základ.

Dohovor č. 108 a všeobecné nariadenie o ochrane údajov pri posudzovaní rozsahu a obmedzení konkrétneho účelu vychádzajú z pojmu zlučiteľnosti: použitie údajov na zlučiteľné účely je povolené na základe pôvodného právneho základu. Ďalšie spracúvanie údajov sa preto nesmie vykonať spôsobom, ktorý je pre dotknutú

287 Pracovná skupina zriadená podľa článku 29 (2013), *Stanovisko 3/2013 k obmedzeniu účelu*, WP 203, 2. apríla 2013.

288 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. b).

osobu neočakávaný, neprimeraný alebo nežiadúci²⁸⁹. Pri posudzovaní toho, či sa má ďalšie spracúvanie považovať za zlučiteľné, by mal prevádzkovateľ zohľadniť (okrem iného):

- „akékoľvek prepojenie medzi týmito účelmi a účelmi zamýšľaného ďalšieho spracúvania,
- kontext, v ktorom sa osobné údaje získali, najmä primerané očakávania dotknutých osôb vyplývajúce z ich vzťahu k prevádzkovateľovi, pokiaľ ide o ich ďalšie použitie,
- povahu osobných údajov,
- následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby, a
- existenciu primeraných záruk v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania²⁹⁰. To sa môže zabezpečiť napríklad šifrovaním alebo pseudonymizáciou.

Príklad: Spoločnosť Sunshine získava údaje o zákazníkoch v rámci riadenia vzťahov so zákazníkmi. Následne zasiela tieto údaje spoločnosti Moonlight, ktorá sa venuje priamemu marketingu a ktorá chce tieto údaje použiť na pomoc pri marketingových kampaniach tretích spoločností. Poskytnutie údajov spoločnosti Sunshine na účely marketingu iných spoločností predstavuje následné použitie údajov na nový účel, ktorý nie zlučiteľný s riadením vzťahov so zákazníkmi, teda s pôvodným účelom získavania údajov o zákazníkoch zo strany spoločnosti Sunshine. Poskytnutie údajov spoločnosti Moonlight si teda vyžaduje vlastný právny základ.

Naopak, použitie údajov súvisiacich s riadením vzťahov so zákazníkmi spoločnosťou Sunshine na jej vlastné marketingové účely, na zasielanie marketingových oznámení o jej produktoch jej vlastným zákazníkom sa vo všeobecnosti akceptuje ako zlučiteľný účel.

289 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 49.

290 Všeobecné nariadenie o ochrane údajov, odôvodnenie 50 a článok 6 ods. 4; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 49.

Vo všeobecnom nariadení o ochrane údajov a v modernizovanom Dohovore č. 108 sa uvádza, že „ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely“ sa *a priori* považuje za zlučiteľné s pôvodným účelom²⁹¹. Pri ďalšom spracúvaní osobných údajov sa však musia zaviesť primerané záruky, ako je anonymizácia, šifrovanie alebo pseudonymizácia údajov a obmedzenie prístupu k údajom²⁹². Všeobecné nariadenie o ochrane údajov dopĺňa, že „[a]k dotknutá osoba udelila súhlas alebo sa spracúvanie zakladá na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti, najmä na ochranu dôležitých verejných záujmov, mal by mať prevádzkovateľ možnosť osobné údaje ďalej spracúvať bez ohľadu na zlučiteľnosť účelov“²⁹³. Pri ďalšom spracúvaní by dotknutá osoba mala byť informovaná o jeho účeloch, ako aj o jej právach, ako je právo namietať²⁹⁴.

Príklad: Spoločnosť Sunshine zozbierala a uchováva údaje o svojich zákazníkoch v rámci riadenia vzťahov so zákazníkmi. Ďalšie použitie týchto údajov spoločnosťou Sunshine na účely štatistickej analýzy nákupného správania svojich zákazníkov je prípustné, keďže štatistické účely sú zlučiteľné. Nie je potrebný žiadny dodatočný právny základ, napríklad súhlas dotknutých osôb. Pri ďalšom spracúvaní osobných údajov na štatistické účely však spoločnosť Sunshine musí zaviesť primerané záruky ochrany práv a slobôd dotknutej osoby. Technické a organizačné opatrenia, ktoré musí spoločnosť Sunshine prijať, môžu zahŕňať pseudonymizáciu.

291 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. b); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b). Príkladom takýchto vnútroštátnych ustanovení je [rakúsky zákon o ochrane údajov \(Datenschutzgesetz\)](#), Spolkový úradný vestník I č. 165/1999, § 46.

292 Všeobecné nariadenie o ochrane údajov, článok 6 ods. 4; modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b); dôvodová správa k modernizovanému Dohovoru č. 108, ods. 50.

293 Všeobecné nariadenie o ochrane údajov, odôvodnenie 50.

294 Tamže.

3.3. Zásada minimalizácie údajov

Hlavné body

- Spracúvanie údajov sa musí obmedziť na to, čo je nevyhnutné na splnenie legitímneho účelu.
- Spracúvanie osobných údajov by sa malo uskutočniť len v prípade, že účel spracúvania nie je možné primerane dosiahnuť inými prostriedkami.
- Spracúvanie údajov nesmie neprimerane zasahovať do dotknutých záujmov, práv a slobôd.

Spracúvajú sa len také údaje, ktoré sú „primerané, relevantné a obmedzené vo vzťahu k účelu, na ktorý sa získavajú a/alebo ďalej spracúvajú“²⁹⁵. Kategórie údajov vybraných na spracúvanie musia byť potrebné na dosiahnutie uvedeného celkového cieľa spracovateľských operácií a prevádzkovateľ by mal prísne obmedziť získavanie údajov na také informácie, ktoré sú priamo relevantné na konkrétny účel, ktorý sa spracúvaním sleduje.

Príklad: Vo veci *Digital Rights Ireland*²⁹⁶ SDEÚ posudzoval platnosť smernice o uchovávaní údajov, ktorej cieľom bola harmonizácia vnútroštátnych ustanovení na uchovávanie osobných údajov vytvorených alebo spracúvaných verejne dostupnými elektronickými komunikačnými službami alebo sieťami na ich možné poskytnutie príslušným orgánom na účely boja proti závažnej trestnej činnosti, ako je organizovaná trestná činnosť a terorizmus. Napriek tomu, že sa to považovalo za účel, ktorý skutočne zodpovedá cieľu všeobecného záujmu, všeobecný spôsob, akým sa smernica vzťahovala na „akúkoľvek osobu a všetky spôsoby elektronickej komunikácie, ako aj všetky prevádzkové údaje bez toho, aby stanovovala akékoľvek rozlíšenie, obmedzenie alebo výnimku na základe cieľa, ktorým je boj proti závažnej trestnej činnosti“, sa považoval za problematický²⁹⁷.

²⁹⁵ Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. c), všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. c).

²⁹⁶ SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

²⁹⁷ Tamže, body 44 a 57.

Okrem toho, použitím osobitných technológií na zvyšovanie súkromia je niekedy možné úplne sa vyhnúť použitiu osobných údajov, alebo možno použiť opatrenia na zníženie schopnosti priradovať údaje k dotknutej osobe (napríklad vďaka pseudonymizácii), čo vedie k riešeniam vhodným z hľadiska ochrany súkromia. Tento postup je obzvlášť vhodný v prípade rozsiahlejších systémov spracúvania.

Príklad: Mestská rada ponúka pravidelným používateľom systému mestskej hromadnej dopravy čipovú kartu za určitý poplatok. Meno používateľa je uvedené na povrchu karty, ako aj v elektronickej podobe v čipe. Pri každej jazde autobusom alebo električkou sa čipová karta musí predložiť pred čítacie zariadenie namontované napríklad v autobuse alebo električke. Údaje, ktoré zariadenie prečíta, sa elektronicky porovnajú s databázou obsahujúcou mená osôb, ktoré si zakúpili cestovnú kartu.

Takýto systém nie je optimálny, pokiaľ ide o rešpektovanie zásady minimalizácie údajov: kontrola oprávnenia jednotlivca na jazdu mestskou hromadnou dopravou by sa mohla vykonať bez porovnávania osobných údajov na čipe karty s databázou. Napríklad by stačilo, keby bol v čipe uložený špeciálny elektronický obrázok (napr. čiarový kód), ktorý by po prechode pred čítacím zariadením potvrdil, či je karta platná alebo nie. Takýto systém by nezačlenoval, kto použil aký dopravný prostriedok a kedy. Nezískavali by sa žiadne osobné údaje, čo predstavuje optimálne riešenie v zmysle zásady minimalizácie, keďže dôsledkom tejto zásady je povinnosť minimalizovať získavanie údajov.

V článku 5 ods. 1 modernizovaného Dohovoru č. 108 sa uvádza požiadavka primeranosti pri spracúvaní osobných údajov vo vzťahu k sledovanému legitímnemu účelu. Musí existovať spravodlivá rovnováha medzi všetkými príslušnými záujmami vo všetkých fázach spracúvania. To znamená, že „osobné údaje, ktoré sú primerané a relevantné, ale spôsobili by neprimeraný zásah do príslušných základných práv a slobôd, by sa mali považovať za neprimerané“²⁹⁸.

298 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 52; všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. c).

3.4. Zásada správnosti údajov

Hlavné body

- Zásadu správnosti údajov musí prevádzkovateľ uplatňovať pri všetkých spracovateľských operáciách.
- Nesprávne údaje sa musia bezodkladne vymazať alebo opraviť.
- Údaje môže byť potrebné pravidelne kontrolovať a aktualizovať, aby sa zabezpečila ich správnosť.

Prevádzkovateľ, ktorý disponuje osobnými informáciami, tieto informácie nevyužíva bez toho, aby s primeranou istotou zabezpečil, že údaje sú správne a aktuálne²⁹⁹.

Povinnosť zabezpečiť správnosť údajov je potrebné vnímať v kontexte účelu spracúvania údajov.

Príklad: SDEÚ vo veci *Rijkeboer*³⁰⁰ preskúmal žiadosť holandského štátneho príslušníka o informácie od miestnej správy mesta Amsterdam o totožnosti osôb, ktorým boli v predchádzajúcich dvoch rokoch poskytnuté záznamy o ňom, ktoré má tento miestny orgán k dispozícii, ako aj o obsah poskytnutých údajov. SDEÚ konštatoval, že s „právom na rešpektovanie súkromia je spojená možnosť dotknutej osoby ubezpečiť sa, že jej osobné údaje sa spracovávajú presne a zákonne, konkrétne to znamená, že základné údaje, ktoré sa jej týkajú, sú správne a že sa oznamujú oprávneným príjemcom.“ SDEÚ ďalej odkázal na preambulu smernice o ochrane údajov, v ktorej sa uvádza, že dotknuté osoby musia mať právo na prístup k svojim osobným údajom, aby mohli skontrolovať správnosť údajov³⁰¹.

Môžu sa vyskytnúť aj prípady, keď je aktualizácia uložených údajov z právneho hľadiska zakázaná, pretože účelom ukladania údajov je hlavne dokumentácia udalostí ako historického „momentu“ (snap-shot).

299 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. d); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. d).

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

301 Predtým odôvodnenie 41, preambula smernice 95/46/ES.

Príklad: Záznam o lekárskom zákroku sa nesmie zmeniť, inými slovami aktualizovať, dokonca ani vtedy, keď sa neskôr ukáže, že zistenia uvedené v zázname boli nesprávne. V takejto situácii je možné len doplniť do záznamu dodatky, a to pod podmienkou, že budú jasne vyznačené ako neskoršie príspevky.

Na druhej strane existujú situácie, v ktorých je pravidelná kontrola správnosti údajov a ich aktualizácia absolútne nevyhnutná z dôvodu možnej škody, ktorá by mohla vzniknúť dotknutej osobe v prípade, že by údaje zostali nesprávne.

Príklad: Ak chce niekto uzatvoriť zmluvu o úvere s bankovou inštitúciou, banka zvyčajne skontroluje úverovú bonitu potenciálneho zákazníka. Na tento účel existujú špeciálne databázy obsahujúce údaje o úverovej histórii súkromných osôb. Ak by takáto databáza obsahovala nesprávne alebo zastarané údaje o určitej osobe, mohlo by jej to spôsobiť problémy. Prevádzkovatelia takýchto databáz preto musia vynaložiť osobitné úsilie na dodržanie zásady správnosti.

3.5. Zásada minimalizácie uchovávania

Hlavné body

- Zásada minimalizácie uchovávania znamená, že osobné údaje sa musia vymazať alebo anonymizovať hneď, ako prestanú byť potrebné na účely, na ktoré boli získané.

Podľa článku 5 ods. 1 písm. e) GDPR a podobne podľa článku 5 ods. 4 písm. e) modernizovaného Dohovoru č. 108 sa vyžaduje, aby osobné údaje boli „uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú“. Po dosiahnutí príslušného účelu sa preto údaje musia vymazať alebo anonymizovať. Na tento účel by „prevádzkovateľ mal stanoviť lehoty na vymazanie alebo pravidelné preskúmanie“ s cieľom zabezpečiť, aby sa údaje neuchovávali dlhšie, než je nevyhnutné³⁰².

302 Všeobecné nariadenie o ochrane údajov, odôvodnenie 39.

Vo veci *S. a Marper* ESĽP dospel k záveru, že v rámci základných zásad relevantných nástrojov RE, ako aj podľa právnych predpisov a praxe ďalších zmluvných strán sa požaduje, aby uchovávanie údajov bolo primerané účelu ich zberu a obmedzené v čase, predovšetkým v policajnom sektore³⁰³.

Príklad: Vo veci *S. a Marper*³⁰⁴ ESĽP rozhodol, že neobmedzené uchovávanie odtlačkov prstov, bunkových vzoriek a profilov DNA oboch sťažovateľov je v demokratickej spoločnosti neprimerané a nie je nevyhnutné, keďže trestné konanie proti obom sťažovateľom bolo ukončené zbavením obvinenia a zastavením stíhania.

Časové obmedzenie ukladania osobných údajov sa vzťahuje len na údaje uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb. Zákonné uchovávanie údajov, ktoré už nie sú potrebné, by sa preto mohlo dosiahnuť anonymizáciou údajov.

Pri archivácii údajov na účely verejného záujmu, vedecké alebo historické účely alebo na štatistické účely sa môžu údaje uchovávať na dlhšie obdobia za predpokladu, že takéto údaje sa použijú výlučne na uvedené účely³⁰⁵. Pri pokračujúcom uchovávaní a používaní osobných údajov sa na ochranu práv a slobôd dotknutej osoby musia zaviesť vhodné technické a organizačné opatrenia.

Modernizovaný Dohovor č. 108 tiež povoľuje výnimky zo zásady minimalizácie uchovávania, a to pod podmienkou, že sú stanovené zákonom, rešpektujú podstatu základných práv a slobôd a sú nevyhnutné a primerané na dosiahnutie určitého počtu legitímnych cieľov³⁰⁶. Patria medzi ne okrem iného ochrana národnej bezpečnosti, vyšetrovanie a trestné stíhanie trestných činov, výkon trestných sankcií, ochrana dotknutej osoby a ochrana práv a základných slobôd iných.

303 ESĽP, *S. a Marper/Spojené kráľovstvo* [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008, pozri tiež napríklad: ESĽP, *M.M./Spojené kráľovstvo*, č. 24029/07, 13. novembra 2012.

304 ESĽP, *S. a Marper/Spojené kráľovstvo* [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008.

305 Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. e); modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b) a článok 11 ods. 2.

306 Modernizovaný Dohovor č. 108, článok 11 ods. 1; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 91 – 98.

Príklad: Vo veci *Digital Rights Ireland*³⁰⁷ SDEÚ preskúmal platnosť smernice o uchovávaní údajov, ktorej cieľom bola harmonizácia vnútroštátnych ustanovení na uchovávanie osobných údajov vytvorených alebo spracúvaných verejne dostupnými elektronickými komunikačnými službami alebo sieťami na boj proti závažnej trestnej činnosti, ako je organizovaná trestná činnosť a terorizmus. V smernici o uchovávaní údajov sa stanovuje obdobie uchovávania údajov „minimálne po dobu šiestich mesiacov bez toho, aby sa rozlišovalo medzi kategóriami údajov uvedenými v článku 5 tejto smernice na základe ich prípadného úžitku pre sledovaný cieľ alebo na základe dotknutých osôb“³⁰⁸. SDEÚ sa tiež zaoberal otázkou toho, že v smernici o uchovávaní údajov nie sú uvedené objektívne kritériá na určovanie presného obdobia uchovávania údajov, ktoré môže trvať od najmenej šiestich mesiacov po maximálne 24 mesiacov, aby sa zabezpečilo, že takéto obdobie je obmedzené na to, čo je prísne nevyhnutné³⁰⁹.

3.6. Zásada bezpečnosti údajov

Hlavné body

- Bezpečnosť a dôvernosť osobných údajov sú kľúčovými faktormi pri predchádzaní nepriaznivým účinkom na dotknutú osobu.
- Bezpečnostné opatrenia môžu byť technické a/alebo organizačné.
- Pseudonymizácia je proces, ktorým sa môžu chrániť osobné údaje.
- Primeranosť bezpečnostných opatrení sa musí určiť v každom jednom prípade individuálne a pravidelne sa skúmať.

Podľa zásady bezpečnosti údajov sa vyžaduje, aby pri spracúvaní osobných údajov boli zavedené primerané technické alebo organizačné opatrenia na ochranu údajov pred náhodným, neoprávneným alebo nezákonným prístupom, používaním, úpravou, zverejnením, stratou, zničením alebo poškodením³¹⁰. V GDPR sa uvádza, že

307 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

308 Tamže, bod 63.

309 Tamže, bod 64.

310 Všeobecné nariadenie o ochrane údajov, odôvodnenie 39 a článok 5 ods. 1 písm. f); modernizovaný Dohovor č. 108, článok 7.

prevádzkovateľ a sprostredkovateľ by pri prijímaní takýchto opatrení mali zohľadniť „najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb“³¹¹. V závislosti od konkrétnych okolností každého prípadu by vhodné technické a organizačné opatrenia mohli zahŕňať napríklad pseudonymizáciu a šifrovanie osobných údajov a/alebo pravidelné testovanie a hodnotenie účinnosti opatrení na zaistenie bezpečnosti spracúvania údajov³¹².

Ako sa vysvetľuje v [oddiele 2.1.1](#), pseudonymizácia údajov znamená nahradenie atribútov osobných údajov, ktoré umožňujú identifikáciu dotknutej osoby pseudonymom, pričom na základe technických alebo organizačných opatrení sa tieto atribúty uchovávajú oddelene. Proces pseudonymizácie sa nesmie zamieňať s procesom anonymizácie, v rámci ktorého sa odstránia všetky odkazy umožňujúce identifikáciu osoby.

Príklad: Veta „Karol Novák, narodený 3. apríla 1967, je otcom štyroch detí, dvoch chlapcov a dvoch dievčat“ môže byť pseudonymizovaná napríklad takto:

„K. N. 1967 je otcom štyroch detí, dvoch chlapcov a dvoch dievčat“ alebo

„324 je otcom štyroch detí, dvoch chlapcov a dvoch dievčat“ alebo

„YESz320l je otcom štyroch detí, dvoch chlapcov a dvoch dievčat“.

Používatelia, ktorí budú mať prístup k týmto údajom, zvyčajne nebudú schopní identifikovať „324“ alebo „YESz320l“ ako „Karol Novák, narodený 3. apríla 1967“. Je teda pravdepodobnejšie, že takého údaje nebudú zneužit.

Prvý príklad je však menej bezpečný. Ak bude veta „K. N. 1967 je otcom štyroch detí, dvoch chlapcov a dvoch dievčat“ použitá v malej obci, v ktorej Karol Novák žije, rozpoznanie pána Nováka nemusí byť zložité. Spôsob pseudonymizácie ovplyvňuje účinnosť ochrany údajov.

311 Všeobecné nariadenie o ochrane údajov, článok 32 ods. 1.

312 Tamže.

Osobné údaje so zašifrovanými identifikačnými znakmi sa používajú v mnohých situáciách ako spôsob utajenia totožnosti osôb. To je užitočné najmä v prípadoch, keď prevádzkovatelia musia skontrolovať, či pracujú s rovnakými dotknutými osobami, ale nevyžadujú alebo by nemali mať k dispozícii skutočnú totožnosť dotknutých osôb. Ide napríklad o prípady, keď výskumník skúma priebeh choroby pacientov, ktorých totožnosť pozná len nemocnica, v ktorej sa liečia a z ktorej výskumník získal pseudonymizované chorobopisy. Pseudonymizácia je teda jedným z dôležitých prostriedkov technológií na zvyšovanie súkromia. Môže fungovať ako významná súčasť špecificky navrhutej ochrany súkromia. Znamená to, že ochrana údajov sa stáva súčasťou štruktúry systémov spracúvajúcich údaje.

V článku 25 GDPR, ktorým sa stanovuje špecificky navrhnutá ochrana údajov, sa výslovne uvádza pseudonymizácia ako príklad primeraného technického a organizačného opatrenia, ktoré by prevádzkovatelia mali zaviesť s cieľom zohľadniť zásady ochrany údajov a začleniť nevyhnutné záruky. Prevádzkovatelia tým splnia požiadavky tohto nariadenia a budú chrániť práva dotknutých osôb pri spracúvaní ich osobných údajov.

Dodržiavanie schválených kódexov správania alebo schválených certifikačných mechanizmov sa môže použiť na preukázanie splnenia požiadavky na bezpečnosť spracúvania³¹³. RE vo svojom stanovisku o vplyve spracúvania záznamov o cestujúcich na ochranu údajov uvádza ďalšie príklady vhodných bezpečnostných opatrení na ochranu osobných údajov v systémoch záznamov o cestujúcich. Patrí k nim uchovávanie údajov v bezpečnom fyzickom prostredí, umožnenie kontroly prístupu viacvrstvovým prihlasovaním a ochrana prepájania údajov so silnou kryptografiou³¹⁴.

Príklad: Stránky sociálnych sietí a poskytovatelia e-mailových služieb umožňujú používateľom pridať k službám, ktoré poskytujú, ďalšiu vrstvu na zabezpečenie bezpečnosti údajov, a to zavedením dvojstupňového overenia. Okrem osobného hesla si používatelia musia vybrať aj druhú možnosť prihlásenia do svojho osobného účtu. Môže ísť napríklad o zaslanie bezpečnostného kódu na číslo mobilného telefónu, ktoré je uvedené v osobnom účte. Týmto spôsobom sa v rámci dvojstupňového overovania zabezpečuje lepšia ochrana osobných informácií pred neoprávneným prístupom k osobným účtom prostredníctvom hackerstva.

313 Tamže, článok 32 ods. 3.

314 Rada Európy, Výbor pre Dohovor č. 108, *Stanovisko o dôsledkoch spracúvania záznamov o cestujúcich v oblasti ochrany osobných údajov*, T-PD(2016)18rev, 19. augusta 2016, s. 9.

V dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádzajú ďalšie príklady primeraných záruk, napríklad zavedenie povinnosti služobného tajomstva alebo prijatie kvalifikovaných technických bezpečnostných opatrení, ako je šifrovanie údajov³¹⁵. Pri zavádzaní osobitných bezpečnostných opatrení by mal prevádzkovateľ, alebo prípadne sprostredkovateľ zohľadniť niekoľko prvkov, napríklad povahu a objem spracúvaných osobných údajov, potenciálne nepriaznivé dôsledky pre dotknuté osoby a potrebu obmedzenia prístupu k údajom³¹⁶. Pri zavádzaní primeraných bezpečnostných opatrení sa musí zohľadniť aktuálny stav metód v oblasti bezpečnosti údajov a techník spracúvania údajov. Náklady na takéto opatrenia musia byť úmerné závažnosti a pravdepodobnosti potenciálnych rizík. Bezpečnostné opatrenia sa pravidelne preskúmajú, aby sa mohli podľa potreby aktualizovať³¹⁷.

V prípadoch, keď dôjde k porušeniu ochrany osobných údajov, sa podľa modernizovaného Dohovoru č. 108 aj GDPR od prevádzkovateľa vyžaduje, aby príslušnému dozornému orgánu bezodkladne oznámil porušenie, ktoré povedie k rizikám pre práva a slobody fyzických osôb³¹⁸. Podobná oznamovacia povinnosť voči dotknutej osobe existuje v prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb³¹⁹. Oznamovanie takýchto porušení dotknutým osobám musí byť jasne a jednoducho formulované³²⁰. Ak sa sprostredkovateľ dozvie o porušení ochrany osobných údajov, musí o tom okamžite informovať prevádzkovateľa³²¹. V určitých situáciách sa môžu uplatňovať výnimky z tejto oznamovacej povinnosti. Prevádzkovateľ napríklad nemusí informovať dozorný orgán, ak „nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb“³²². Takisto nie je potrebné informovať dotknutú osobu pri zavedení bezpečnostných opatrení, na základe ktorých sú údaje nečitateľné pre neoprávnené osoby, alebo ak sa následnými opatreniami zabezpečí, že vysoké riziko pravdepodobne už nebude mať dôsledky³²³. Ak by si oznámenie porušenia ochrany osobných údajov dotknutým osobám vyžadovalo vynaloženie neprimeraného úsilia zo strany prevádzkovateľa, v takom prípade dôjde

315 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 56.

316 Tamže, bod 62.

317 Tamže, bod 63.

318 Modernizovaný Dohovor č. 108, článok 7 ods. 2, všeobecné nariadenie o ochrane údajov, článok 33 ods. 1.

319 Modernizovaný Dohovor č. 108, článok 7 ods. 2, všeobecné nariadenie o ochrane údajov, článok 34 ods. 1.

320 Všeobecné nariadenie o ochrane údajov, článok 34 ods. 2.

321 Tamže, článok 33 ods. 1.

322 Tamže.

323 Tamže, článok 34 ods. 3 písm. a) a písm. b).

namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že „dotknuté osoby budú informované rovnako efektívnym spôsobom“³²⁴.

3.7. Zásada zodpovednosti

Hlavné body

- Zodpovednosť si vyžaduje, aby prevádzkovatelia a sprostredkovatelia aktívne a priebežne prijímali opatrenia na podporu a zabezpečenie ochrany údajov pri spracovateľských činnostiach.
- Prevádzkovatelia a sprostredkovatelia sú zodpovední za súlad svojich spracovateľských operácií s právnymi predpismi o ochrane údajov a ich príslušnými povinnosťami.
- Prevádzkovatelia musia byť kedykoľvek schopní preukázať súlad s ustanoveniami o ochrane údajov dotknutým osobám, širokej verejnosti a dozorným orgánom. Sprostredkovatelia musia tiež spĺňať niektoré povinnosti, ktoré sú úzko spojené so zodpovednosťou (napríklad vedenie záznamov o spracovateľských operáciách a určenie zodpovednej osoby).

V GDPR a modernizovanom Dohovore č. 108 sa stanovuje, že prevádzkovateľ je zodpovedný za zásady spracúvania osobných údajov opísané v tejto kapitole a musí byť schopný preukázať ich dodržiavanie³²⁵. Na tento účel musí prevádzkovateľ zaviesť primerané technické a organizačné opatrenia³²⁶. Hoci sa zásada zodpovednosti podľa článku 5 ods. 2 GDPR zameriava len na prevádzkovateľov, očakáva sa, že sprostredkovatelia budú takisto zodpovední, keďže musia spĺňať viaceré povinnosti a zodpovednosť sa ich úzko dotýka.

V právnych predpisoch EÚ a RE o ochrane údajov sa takisto stanovuje, že prevádzkovateľ je zodpovedný za dodržiavanie zásad ochrany údajov uvedených v [oddieloch 3.1 až 3.6](#) a mal by byť schopný zabezpečiť ich dodržiavanie³²⁷. Pracovná skupina zriadená podľa článku 29 uvádza, že „druhy postupov a mechanizmov by sa mali meniť podľa rizík, ktoré predstavuje spracúvanie a povaha údajov“³²⁸.

324 Tamže, článok 34 ods. 3 písm. c).

325 Tamže, článok 5 ods. 2; modernizovaný Dohovor č. 108, článok 10 ods. 1.

326 Všeobecné nariadenie o ochrane údajov, článok 24.

327 Tamže, článok 5 ods. 2; modernizovaný Dohovor č. 108, článok 10 ods. 1.

328 Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 3/2010 k zásade zodpovednosti*, WP 173, Brusel, 13. júla 2010, bod 12.

Prevádzkovatelia si môžu uľahčiť plnenie tejto požiadavky rôznymi spôsobmi, medzi ktoré patria:

- vedenie záznamov o spracovateľských činnostiach a na požiadanie ich sprístupnenie dozornému orgánu³²⁹,
- v určitých situáciách určenie zodpovednej osoby, ktorá je zapojená do všetkých otázok týkajúcich sa ochrany osobných údajov³³⁰,
- vykonanie posúdenia vplyvu na ochranu údajov pre typy spracúvania, ktoré by mohli viesť k vysokému riziku pre práva a slobody fyzických osôb³³¹,
- zabezpečenie špecificky navrhutej a štandardnej ochrany osobných údajov³³²,
- zavedenie postupov a procesov na uplatňovanie práv dotknutých osôb³³³,
- dodržiavanie schválených kódexov správania alebo certifikačných mechanizmov³³⁴.

Hoci sa zásada zodpovednosti uvedená v článku 5 ods. 2 GDPR nevzťahuje konkrétne na sprostredkovateľov, existujú ustanovenia spojené so zodpovednosťou, ktoré obsahujú aj povinnosti pre sprostredkovateľov, ako je vedenie záznamov o spracovateľských činnostiach a určenie zodpovednej osoby pre všetky spracovateľské činnosti, pri ktorých je potrebná³³⁵. Sprostredkovatelia musia tiež zabezpečiť vykonanie všetkých opatrení potrebných na zaistenie bezpečnosti údajov³³⁶. V právne záväznej zmluve medzi prevádzkovateľom a sprostredkovateľom sa musí stanoviť, že sprostredkovateľ pomáha prevádzkovateľovi pri zabezpečovaní súladu s niektorými požiadavkami, napríklad pri vykonávaní posúdenia vplyvu na ochranu údajov alebo pri informovaní prevádzkovateľa o akomkoľvek porušení ochrany osobných údajov, hneď ako sa o ňom dozvie³³⁷.

329 Všeobecné nariadenie o ochrane údajov, článok 30.

330 Tamže, článok 37 až 39.

331 Tamže, článok 35; modernizovaný Dohovor č. 108, článok 10 ods. 2.

332 Všeobecné nariadenie o ochrane údajov, článok 25; modernizovaný Dohovor č. 108, článok 10 ods. 2 a 3.

333 Tamže, článok 12 a článok 24.

334 Tamže, článok 40 a článok 42.

335 Tamže, článok 5 ods. 2, články 30 a 37.

336 Tamže, článok 28 ods. 3 písm. c).

337 Tamže, článok 28 ods. 3 písm. d).

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) prijala v roku 2013 usmernenia o ochrane súkromia, v ktorých zdôraznila, že prevádzkovatelia zohrávajú dôležitú úlohu pri zabezpečovaní ochrany údajov v praxi. V usmerneniach je uvedená zásada zodpovednosti, z ktorej vyplýva že „prevádzkovateľ by mal byť zodpovedný za súlad s opatreniami, ktoré zaisťujú realizáciu uvedených [vecných] zásad“³³⁸.

Príklad: Legislatívnym príkladom, ktorý zdôrazňuje zásadu zodpovednosti, je zmena smernice 2002/58/ES o súkromí a elektronických komunikáciách z roku 2009³³⁹. Podľa článku 4 zmeneného znenia smernice sa ukladá povinnosť zabezpečenia „vykonávania bezpečnostnej politiky vo vzťahu k spracovaniu osobných údajov“. Pokiaľ ide o bezpečnostné ustanovenia uvedenej smernice, zákonodarcu rozhodol, že je nevyhnutne potrebné uviesť výslovnú požiadavku vypracovať a vykonávať bezpečnostnú politiku.

Podľa stanoviska pracovnej skupiny zriadenej podľa článku 29³⁴⁰ je podstatou zodpovednosti povinnosť prevádzkovateľa:

- zaviesť opatrenia, ktoré by za bežných okolností zaručovali dodržiavanie pravidiel ochrany údajov v súvislosti so spracovateľskými operáciami; a
- mať pripravenú dokumentáciu, ktorá preukáže dotknutým osobám a dozorným orgánom opatrenia, ktoré boli prijaté na dosiahnutie súladu s pravidlami ochrany údajov.

Pri zásade zodpovednosti sa preto vyžaduje, aby prevádzkovatelia aktívne preukazovali súlad a nečakali na to, aby dotknuté osoby alebo dozorné orgány zistili nedostatky.

338 OECD (2013), *Usmernenia o riadení ochrany súkromia a cezhraničných tokov osobných údajov*, článok 14.

339 Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, Ú. v. EÚ L 337, 2009, s. 11.

340 Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 3/2010 k zásade zodpovednosti*, WP 173, Brusel, 13. júla 2010.

4

Pravidlá európskych právných predpisov o ochrane údajov

EÚ	Zahrnuté témy	RE
Pravidlá zákonného spracúvania údajov		
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. a) SDEÚ, C-543/09, <i>Deutsche Telekom AG/Bundesrepublik Deutschland</i> , 2011 SDEÚ, C-536/15, <i>Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)</i> , 2017	Súhlas	Odporúčanie o profilovaní Článok 3.4 bod b) a článok 3.6 Modernizovaný Dohovor č. 108, článok 5 ods. 2
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. b)	(Pred)-zmluvný vzťah	Odporúčanie o profilovaní, článok 3.4 písm. b)
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. c)	Zákonné povinnosti prevádzkovateľa	Odporúčanie o profilovaní, článok 3.4 písm. a)
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. d)	Životne dôležité záujmy dotknutej osoby	Odporúčanie o profilovaní, článok 3.4 písm. b)
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. e) SDEÚ, C-524/06, <i>Huber/Bundesrepublik Deutschland [VK]</i> , 2008	Verejný záujem a výkon verejnej moci	Odporúčanie o profilovaní, článok 3.4 písm. b)

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. f) SDEÚ, C-13/16, <i>Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme”, 2017</i> SDEÚ, spojené veci C-468/10 a C-469/10, <i>Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado</i> , 2011	Oprávnené záujmy iných	Odporúčanie o profilovaní, článok 3.4 písm. b) ESLP, <i>Y/Turecko</i> , č. 648/10, 2015
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 4	Výnimka z obmedzenia účelu: ďalšie spracúvanie na iné účely	Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b)
Pravidlá zákonného spracúvania citlivých údajov		
Všeobecné nariadenie o ochrane údajov, článok 9 ods. 1	Všeobecný zákaz spracúvania	Modernizovaný Dohovor č. 108, článok 6
Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2	Výnimky zo všeobecného zákazu	Modernizovaný Dohovor č. 108, článok 6
Pravidlá bezpečného spracúvania		
Všeobecné nariadenie o ochrane údajov, článok 32	Povinnosť zabezpečiť bezpečné spracúvanie	Modernizovaný Dohovor č. 108, článok 7 ods. 1 ESLP, <i>I/Fínsko</i> , č. 20511/03, 2008
Všeobecné nariadenie o ochrane údajov, článok 28 a článok 32 ods. 1 písm. b)	Povinnosť zachovávať dôvernosť	Modernizovaný Dohovor č. 108, článok 7 ods. 1
Všeobecné nariadenie o ochrane údajov, článok 34 Smernica o súkromí a elektronických komunikáciách, článok 4 ods. 2	Oznámenia o porušení ochrany údajov	Modernizovaný Dohovor č. 108, článok 7 ods. 2
Pravidlá týkajúce sa zodpovednosti a podpory súladu		
Všeobecné nariadenie o ochrane údajov, články 12, 13 a 14	Transparentnosť vo všeobecnosti	Modernizovaný Dohovor č. 108, článok 8
Všeobecné nariadenie o ochrane údajov, články 37, 38 a 39	Zodpovedné osoby	Modernizovaný Dohovor č. 108, článok 10 ods. 1
Všeobecné nariadenie o ochrane údajov, článok 30	Záznamy o spracovateľských činnostiach	
Všeobecné nariadenie o ochrane údajov, články 35 a 36	Posúdenie vplyvu a predchádzajúca konzultácia	Modernizovaný Dohovor č. 108, článok 10 ods. 2

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, články 33 a 34	Oznámenia o porušení ochrany údajov	Modernizovaný Dohovor č. 108, článok 7 ods. 2
Všeobecné nariadenie o ochrane údajov, články 40 a 41	Kódexy správania	
Všeobecné nariadenie o ochrane údajov, články 42 a 43	Certifikácia	
Špecificky navrhnutá a štandardná ochrana údajov		
Všeobecné nariadenie o ochrane údajov, článok 25 ods. 1	Špecificky navrhnutá ochrana údajov	Modernizovaný Dohovor č. 108, článok 10 ods. 2
Všeobecné nariadenie o ochrane údajov, článok 25 ods. 2	Štandardná ochrana údajov	Modernizovaný Dohovor č. 108, článok 10 ods. 3

Zásady sú spravidla všeobecnej povahy. Pri ich uplatňovaní v konkrétnych situáciách sa ponecháva určitý priestor na interpretáciu a výber prostriedkov. V **právnych predpisoch RE** sa zmluvným stranám modernizovaného Dohovoru č. 108 prenecháva, aby tento priestor na interpretáciu objasnili vo svojich vnútroštátnych právnych predpisoch. V **právnych predpisoch EÚ** sa naopak v záujme zabezpečenia ochrany údajov na vnútornom trhu považovalo za potrebné mať na úrovni EÚ podrobnejšie pravidlá na harmonizáciu úrovne ochrany údajov vo vnútroštátnych právnych predpisoch členských štátov. Vo všeobecnom nariadení o ochrane údajov a stanovuje vrstva podrobných pravidiel podľa zásad stanovených v jeho článku 5, ktoré sú priamo uplatniteľné v právnych poriadkoch jednotlivých členských štátov. Nasledujúci text o podrobných pravidlách ochrany údajov na európskej úrovni sa preto prevažne zaoberá právnymi predpismi EÚ.

4.1. Pravidlá zákonného spracúvania

Hlavné body

- Osobné údaje sa môžu zákonne spracúvať, ak spĺňajú jedno z týchto kritérií:
 - spracúvanie je založené na súhlase dotknutej osoby,
 - zmluvný vzťah si vyžaduje spracúvanie osobných údajov,
 - spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa,

- životne dôležité záujmy dotknutých osôb alebo inej osoby si vyžadujú spracúvanie ich údajov,
- spracúvanie potrebné na splnenie úlohy realizovanej vo verejnom záujme,
- oprávnené záujmy prevádzkovateľov alebo tretích strán sú dôvodom spracúvania, ale len keď nad nimi neprevážujú záujmy alebo základné práva dotknutých osôb.
- Na zákonné spracúvanie citlivých osobných údajov sa vzťahuje osobitný, prísnejší režim.

4.1.1. Právne základy spracúvania údajov

V kapitole II všeobecného nariadenia o ochrane údajov s názvom „Zásady“ sa stanovuje, že spracúvanie osobných údajov musí v prvom rade spĺňať zásady týkajúce sa kvality údajov stanovené v článku 5 GDPR. Jednou zo zásad je, že osobné údaje by sa mali spracúvať „zákonným spôsobom, spravodlivo a transparentne“. Po druhé, aby sa údaje spracúvali zákonným spôsobom, spracúvanie musí byť v súlade s jedným z právnych základov na to, aby bolo spracúvanie údajov legítimne – sú uvedené v článku 6³⁴¹ pre osobné údaje, ktoré nemajú citlivý charakter, a v článku 9 pre osobitné kategórie údajov (alebo citlivé údaje). Podobne v kapitole II modernizovaného Dohovoru č. 108, v ktorej sa stanovujú „základné zásady ochrany osobných údajov“, sa uvádza, že na to, aby bolo spracúvanie údajov zákonné, musí byť „primerané vo vzťahu k sledovanému legítimnému účelu“.

Bez ohľadu na právny základ spracúvania, ktorý prevádzkovateľ uplatňuje pri začatí spracovateľskej operácie osobných údajov, prevádzkovateľ bude musieť uplatňovať aj záruky stanovené vo všeobecnom systéme práva v oblasti ochrany údajov.

Súhlas

V právnych predpisoch RE sa súhlas spomína v článku 5 ods. 2 modernizovaného Dohovoru č. 108. Na súhlas sa odkazuje aj v judikatúre ESĽP a viacerých

341 SDEÚ, spojené veci C-465/00, C-138/01 a C-139/01, *Rechnungshof/Österreichischer Rundfunk a i. a Christa Neukomm a Joseph Lauermaun/Österreichischer Rundfunk*, 20. mája 2003, bod. 65; SDEÚ, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008, bod. 48; SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECMD)/Administración del Estado*, 24. novembra 2011, bod 26.

odporúčaniach Rady Európy³⁴². **Podľa právnych predpisov EÚ** je súhlas ako základ pre zákonné spracúvanie údajov pevne stanovený v článku 6 GDPR a výslovne sa uvádza aj v článku 8 Charty. Znak platného súhlasu sú vysvetlené vo vymedzení tohto pojmu v článku 4 všeobecného nariadenia o ochrane údajov, zatiaľ čo podmienky získania platného súhlasu sú podrobne uvedené v článku 7 a osobitné pravidlá pre súhlas dieťaťa v súvislosti so službami informačnej spoločnosti sa stanovujú v článku 8 GDPR.

Ako je vysvetlené v **oddiele 2.4**, súhlas musí byť slobodne daný, informovaný, konkrétny a jednoznačný. Súhlas musí byť vyhlásenie alebo jednoznačný potvrdzujúci úkon, ktorým sa vyjadruje súhlas so spracúvaním, a osoba má právo kedykoľvek svoj súhlas odvolať. Prevádzkovatelia majú povinnosť uchovávať overiteľný záznam o súhlase.

Slobodný súhlas

V rámci právneho systému **RE**, ktorý tvorí modernizovaný Dohovor č. 108, musí súhlas dotknutej osoby „predstavovať slobodné vyjadrenie úmyselného výberu“³⁴³. Slobodný súhlas môže byť platný len vtedy, „ak si dotknutá osoba skutočne môže vybrať a neexistuje riziko podvodu, zastrašovania, nátlaku alebo významných negatívnych následkov, ak dotknutá osoba nebude súhlasiť“³⁴⁴. V tejto súvislosti sa v **právnych predpisoch EÚ** stanovuje, že súhlas sa nepovažuje za slobodný, „ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu alebo nemôže odmietnuť či odvolať súhlas bez nepriaznivých následkov“³⁴⁵. V GDPR sa zdôrazňuje, že „[p]ri posudzovaní, či bol súhlas poskytnutý slobodne, sa v čo najväčšej miere okrem iného zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný“³⁴⁶. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza, že „na dotknutú osobu by sa nemal vyvíjať žiadny neprimeraný vplyv alebo tlak (ktorý môže mať hospodársku alebo inú povahu), či už priamy, alebo nepriamy,

342 Pozri napríklad Rada Európy, Výbor ministrov (2010), Odporúčanie Rec(2010)13 členským štátom o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania, 23. novembra 2010, článok 3.4 písm. b).

343 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42.

344 Pozri tiež: Pracovná skupina zriadená podľa článku 29 (2011), *Stanovisko 15/2011 k definícii súhlasu*, WP 187, Brusel, 13. júla 2011, s. 12.

345 Všeobecné nariadenie o ochrane údajov, odôvodnenie 42.

346 Tamže, článok 7 ods. 4.

a súhlas by sa nemal považovať za slobodný, ak dotknutá osoba nemá skutočnú voľbu alebo nie je schopná odmietnuť alebo odvolať súhlas bez následkov”³⁴⁷.

Príklad: Niektoré obce v štáte A sa rozhodli vytvoriť pobytové preukazy so zabudovaným čipom. Získanie týchto elektronických kariet nie je pre obyvateľov obce povinné. Obyvatelia, ktorí nevlastnia kartu, však nemajú prístup k viacerým dôležitým službám verejnej správy, ako je možnosť platiť obecné dane online, podávať sťažnosti elektronicky a využiť trojdňovú lehotu na získanie odpovede, a dokonca možnosť nemusieť čakať v rade, zakúpiť si zľavnené vstupenky pri návšteve koncertnej haly a použiť skenery pri vstupe.

Spracúvanie osobných údajov zo strany obcí v tomto prípade nemôže byť založené na súhlase. Vzhľadom na to, že existuje aspoň nepriamy tlak na obyvateľov, aby získali elektronickú kartu a súhlasili so spracúvaním, súhlas nie je poskytnutý slobodne. Obce by preto systémy elektronických kariet mali vytvárať na základe iného legitímneho dôvodu na spracúvanie. Mohli by napríklad vychádzať z toho, že spracúvanie je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme, čo predstavuje právny základ pre spracúvanie podľa článku 6 ods. 1 písm. e) GDPR³⁴⁸.

Slobodný súhlas by mohol byť spochybnený aj v prípade podriadenosti, ak existuje významná hospodárska alebo iná nerovnováha medzi prevádzkovateľom, ktorý získava súhlas a dotknutou osobou, ktorá poskytuje súhlas³⁴⁹. Typickým príkladom takejto nerovnováhy a podriadenosti je spracúvanie osobných údajov zo strany zamestnávateľa v rámci pracovnoprávneho vzťahu. Podľa pracovnej skupiny zriadenej podľa článku 29 „[z]amestnanci takmer nikdy nie sú v postavení, v ktorom by mohli slobodne udeliť, zamietnuť alebo zrušiť súhlas vzhľadom na závislosť vyplývajúcu zo vzťahu medzi zamestnávateľom a zamestnancom. Zamestnanci môžu

347 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42.

348 Pracovná skupina zriadená podľa článku 29 (2011), *Stanovisko 15/2011 k definícii súhlasu*, WP 187, Brusel, 13. júla 2011, s. 16. Ďalšie príklady prípadov, keď spracúvanie údajov nemôže byť založené na súhlase, ale vyžaduje si iný právny základ na to, aby bolo zákonné, možno nájsť na stranách 14 a 17 stanoviska.

349 Pozri tiež pracovná skupina zriadená podľa článku 29 (2001), *Stanovisko 8/2001 k spracúvaniu osobných údajov v súvislosti s pracovným pomerom*, WP 48, Brusel, 13. septembra 2001; pracovná skupina zriadená podľa článku 29 (2005), pracovný dokument o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995, WP 114, Brusel, 25. novembra 2005; pracovná skupina zriadená podľa článku 29 (2017), *Stanovisko č. 2/2017 k spracúvaniu údajov v práci*, WP 249, Brusel, 8. júna 2017.

vzhľadom na nerovnováhu moci dať slobodný súhlas iba za mimoriadnych okolností, keď s prijatím alebo zamietnutím ponuky nie sú spojené vôbec nijaké následky”³⁵⁰.

Príklad: Veľká spoločnosť plánuje vytvoriť adresár obsahujúci mená všetkých zamestnancov, ich funkcie v rámci spoločnosti a služobné adresy výlučne na účely zlepšenia vnútropodnikovej komunikácie. Vedúci personálneho oddelenia navrhne pridať do adresára fotografie jednotlivých zamestnancov, aby sa uľahčilo rozpoznávanie kolegov na stretnutiach. Zástupcovia zamestnancov požadujú, aby pridanie fotografie bolo podmienené súhlasom jednotlivých zamestnancov.

V takom prípade by sa súhlas zamestnanca mal pokladať za právny základ spracúvania fotografií v adresári, keďže sa dá očakávať, že ak zamestnanec odmietne uverejnenie svojej fotografie v adresári, nebude to preňho mať žiadne negatívne dôsledky zo strany zamestnávateľa.

Príklad: Spoločnosť A plánuje stretnutie troch svojich zamestnancov s riadiacimi pracovníkmi spoločnosti B s cieľom prediskutovať potenciálnu budúcu spoluprácu na projekte. Stretnutie sa uskutoční v priestoroch spoločnosti B, ktorá od spoločnosti A požaduje, aby jej e-mailom zaslala mená, životopisy a fotografie účastníkov stretnutia. Spoločnosť B tvrdí, že potrebuje mená a fotografie účastníkov, aby zamestnanci bezpečnostnej služby pri vstupe do budovy mohli skontrolovať, či ide o správne osoby, zatiaľ čo životopisy umožnia riadiacim pracovníkom lepšie sa pripraviť na stretnutie. V tomto prípade nemôže byť poskytnutie osobných údajov zamestnancov spoločnosti A založené na súhlase. Súhlas nemožno považovať za „slobodný“, keďže je možné, že zamestnanci môžu čeliť negatívnym dôsledkom, ak súhlas neposkytnú (napríklad ich môže nahradiť iný kolega, ktorý sa nezúčastní len na stretnutí, ale aj na spolupráci so spoločnosťou B a všeobecne na projekte). Preto sa spracúvanie musí zakladať na inom právnom základe.

To však neznamená, že súhlas nikdy nemôže byť platný za okolností, keď by jeho odmietnutie malo negatívne dôsledky. Napríklad, ak nesúhlas s vystavením zákaznickej karty v supermarkete vedie len k tomu, že zákazník nemá nárok na zníženie ceny určitého tovaru, súhlas zostáva platným právnym základom na spracúvanie

350 Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 2/2017 k spracúvaniu údajov v práci*, WP 249, Brusel, 8. júna 2017.

osobných údajov tých zákazníkov, ktorí súhlasili s vystavením takejto karty. Medzi zákazníkom a supermarketom neexistuje vzťah podriadenosti a dôsledky neposkytnutia súhlasu nie sú natoľko závažné, aby dotknutej osobe bránili v slobodnom výbere (za predpokladu, že zníženie ceny nie je dostatočné na to, aby ovplyvnilo slobodný výber).

Ak sa však tovar alebo služby dajú získať len pod podmienkou poskytnutia určitých osobných údajov prevádzkovateľovi alebo ďalším tretím stranám, súhlas dotknutej osoby so zverejnením jej údajov, ktoré nie sú potrebné na uzatvorenie zmluvy, nie je možné pokladať za slobodné rozhodnutie, a preto podľa právnych predpisov o ochrane údajov nie je platný³⁵¹. GDPR je dosť prísne, pokiaľ ide o zákaz podmienenia poskytovania tovaru a služieb poskytnutím súhlasu³⁵².

Príklad: Súhlas cestujúcich s tým, aby letecká spoločnosť poskytla tzv. záznamy o cestujúcich, t. j. údaje o ich totožnosti, stravovacích návykoch alebo zdravotných problémoch, imigračným orgánom konkrétneho cudzieho štátu, nemožno pokladať za platný súhlas podľa právnych predpisov o ochrane údajov, keďže cestujúci nemajú na výber, ak chcú navštíviť danú krajinu. Ak má byť poskytnutie takýchto údajov zákonné, je potrebný iný právny základ než súhlas: s najväčšou pravdepodobnosťou osobitný právny predpis.

Informovaný súhlas

Dotknutá osoba musí mať pred prijatím rozhodnutia dostatok informácií. Informovaný súhlas zvyčajne obsahuje presný a ľahko zrozumiteľný opis záležitosti, ktorá si vyžaduje súhlas. Ako vysvetľuje pracovná skupina zriadená podľa článku 29, súhlas sa musí zakladať na zhodnutí a pochopení skutočností a dôsledkov úkonu poskytnutia súhlasu so spracúvaním. „Príslušnej osobe sa musia jasným a zrozumiteľným spôsobom poskytnúť presné a úplné informácie o všetkých príslušných záležitostiach [...], napríklad povaha spracúvaných údajov, účely spracúvania, možní príjemcovia a práva dotknutej osoby“³⁵³. Na to, aby bol súhlas informovaný, jednotlivci musia vedieť aj o dôsledkoch neposkytnutia súhlasu so spracúvaním údajov.

351 Všeobecné nariadenie o ochrane údajov, článok 7 ods. 4.

352 Tamže.

353 Pracovná skupina zriadená podľa článku 29 (2007), pracovný dokument o spracovaní osobných údajov týkajúcich sa zdravotného stavu v elektronických zdravotných záznamoch (EZZ), WP 131, Brusel, 15. februára 2007.

Vzhľadom na význam informovaného súhlasu sa v GDPR a v dôvodovej správe k modernizovanému Dohovoru č. 108 tento pojem objasňuje. V odôvodneniach GDPR sa stanovuje, že „dotknutá osoba by si mala byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov“³⁵⁴.

Vo výnimočnom prípade, ak sa súhlas používa ako výnimka na zabezpečenie právneho základu pre medzinárodný prenos údajov, tento súhlas sa považuje za platný len vtedy, ak prevádzkovateľ informuje dotknutú osobu o možných rizikách, ktoré takéto prenosi môžu pre ňu predstavovať vzhľadom na neexistenciu rozhodnutia o primeranosti a primeraných záruk³⁵⁵.

V dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza, že sa musia poskytnúť informácie o dôsledkoch rozhodnutia dotknutej osoby, a o tom, „čo poskytnutie súhlasu zahŕňa a o rozsahu, v ktorom sa súhlas udeľuje“³⁵⁶.

Kvalita informácií je dôležitá. Kvalita informácií znamená, že jazyk informácie by sa mal prispôbiť predpokladanému príjemcovi. Informácie sa musia poskytnúť bez žargónu, v jasnom a jednoduchom jazyku, ktorému by mal bežný používateľ byť schopný rozumieť³⁵⁷. Informácie musia byť dotknutej osobe ľahko dostupné a môžu sa poskytnúť ústne alebo písomne. Prístupnosť a viditeľnosť informácií sú dôležitými prvkami: informácie musia byť jasne viditeľné a nápadné. V online prostredí môžu byť dobrým riešením aj vrstvené upozornenia, pretože umožňujú dotknutým osobám vybrať si prístup k stručnej alebo rozsiahlejšej verzii informácií.

Konkrétny súhlas

Aby bol súhlas platný, musí sa týkať konkrétneho účelu spracúvania, ktorý musí byť jasne a jednoznačne opísaný. Súvisí to s kvalitou informácií poskytnutých o účele súhlasu. V tejto súvislosti budú relevantné primerané očakávania priemernej dotknutej osoby. Dotknutá osoba musí byť požiadaná o nový súhlas, ak sa spracovateľské operácie pridávajú alebo menia spôsobom, ktorý nebolo možné odôvodnene predpokladať, keď bol udelený pôvodný súhlas, a teda viedli k zmene účelu. Ak sa spracúvanie vykonáva na viaceré účely, súhlas by sa mal udeliť na všetky tieto účely³⁵⁸.

354 Všeobecné nariadenie o ochrane údajov, odôvodnenie 42.

355 Tamže, článok 49 ods. 1 písm. a).

356 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 42.

357 Pracovná skupina zriadená podľa článku 29 (2011), *Stanovisko 15/2011 k definícii súhlasu*, WP 187, Brusel, 13. júla 2011, s. 19.

358 Všeobecné nariadenie o ochrane údajov, odôvodnenie 32.

Príklady: SDEÚ sa vo veci *Deutsche Telekom AG*³⁵⁹ zaoberal otázkou, či poskytovateľ telekomunikačných služieb, ktorý musel postúpiť osobné údaje účastníkov na zverejnenie v telefónnych zoznamoch, potreboval nový súhlas od dotknutých osôb³⁶⁰, keďže pri poskytnutí pôvodného súhlasu neboli uvedení príjemcovia údajov.

SDEÚ dospel k záveru, že podľa článku 12 smernice o súkromí a elektronických komunikáciách nebolo pred postúpením údajov potrebné získavať nový súhlas. Dotknuté osoby mali len možnosť vyjadriť súhlas s účelom spracúvania, ktorým bolo uverejnenie ich údajov, a nemohli si vybrať rôzne telefónne zoznamy, v ktorých by tieto údaje mohli byť uverejnené.

SDEÚ zdôraznil, že „z kontextového a systematického výkladu článku 12 smernice o súkromí a elektronických komunikáciách vyplýva, že sa súhlas v zmysle druhého odseku tohto článku vzťahuje na účel zverejnenia osobných údajov vo verejnom zozname, a nie na totožnosť konkrétneho poskytovateľa zoznamu“³⁶¹. Okrem toho účastníka nepoškodí informácia o totožnosti autora zverejnenia, ale „samotné zverejnenie osobných údajov v telefónnom zozname, ktorý má osobitný účel“³⁶².

Vec *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV/Autoriteit Consument en Markt (AMC)*³⁶³ sa týkala požiadavky belgickej spoločnosti, ktorá poskytuje telefónne informačné služby a služby telefónnych zoznamov pre spoločnosti, ktoré pridávajú telefónne čísla v Holandsku, aby jej poskytli prístup k údajom týkajúcim sa ich účastníkov. Belgická spoločnosť sa odvolávala na povinnosť vyplývajúcu zo smernice univerzálnej služby³⁶⁴. Od spoločností, ktoré pridávajú telefónne čísla, sa tu vyžaduje, aby sprístupnili telefónne čísla pre telefónne zoznamy, ktoré ich požadujú, ak účastníci súhlasili s tým, aby

359 SDEÚ, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5. mája 2011. Pozri najmä body 53 a 54.

360 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávanía osobných údajov a ochrany súkromia v sektore elektronických komunikácií, Ú. v. ES L 201, 2002 (smernica o súkromí a elektronických komunikáciách).

361 SDEÚ, C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5. mája 2011, bod 61.

362 Tamže, bod 62.

363 SDEÚ, C-536/15, *Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)*, 15. marca 2017.

364 Smernica Európskeho parlamentu a Rady 2002/22/ES zo 7. marca 2002 o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb (smernica univerzálnej služby), Ú. v. ES L 108, 2002, s. 51, zmenená smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (smernica univerzálnej služby), Ú. v. EÚ L 337, 2009, s. 11.

ich čísla boli zverejnené. Holandské spoločnosti to odmietli, pričom uviedli, že nie sú povinné poskytnúť predmetné údaje podniku usadenému v inom členskom štáte. Tvrdili, že používatelia vyjadrili súhlas s uverejnením svojich čísel za predpokladu, že budú uverejnené v holandskom telefónnom zozname. SDEÚ skonštatoval, že smernica univerzálnej služby sa vzťahuje na všetky žiadosti spoločností poskytujúcich telefónne informačné služby bez ohľadu na to, v ktorom členskom štáte sú usadené. SDEÚ tiež rozhodol, že sprístupnenie tých istých údajov inému podniku s cieľom ich zverejnenia vo verejnom zozname bez získania nového súhlasu od týchto účastníkov nemôže zasahovať do samotnej podstaty práva na ochranu osobných údajov³⁶⁵. Preto nie je potrebné, aby podnik, ktorý svojim účastníkom prideliuje telefónne čísla, formuloval svoju žiadosť o súhlas adresovanú účastníkovi tak, aby tento účastník vyjadril svoj súhlas osobitne podľa toho, do ktorého členského štátu sa údaje, ktoré sa ho týkajú, môžu zaslať³⁶⁶.

Jednoznačný súhlas

Každý súhlas sa musí udeliť jednoznačným spôsobom³⁶⁷. To znamená, že by nemali existovať žiadne opodstatnené pochybnosti o tom, že dotknutá osoba chcela vyjadriť súhlas so spracúvaním svojich údajov. Napríklad nečinnosť zo strany dotknutej osoby sa nepovažuje za jednoznačný súhlas.

Vzťahuje sa to na prípady, keď prevádzkovateľ získava súhlas formou vyhlásenia v politike ochrany súkromia, ako napríklad „použitím našej služby udeľujete súhlas so spracúvaním vašich osobných údajov“. V takom prípade prevádzkovatelia musia zabezpečiť, aby používatelia mohli manuálne a individuálne súhlasiť s takýmito pravidlami.

Ak sa súhlas udeľuje v písomnej forme, ktorá je súčasťou zmluvy, súhlas so spracúvaním osobných údajov musí byť individualizovaný a v každom prípade „by záruky mali zabezpečovať, že dotknutá osoba si je vedomá, že dáva súhlas a v akom rozsahu ho udeľuje“³⁶⁸.

365 SDEÚ, C-536/15, *Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)*, 15. marca 2017, bod 36.

366 Tamže, body 40 – 41.

367 Všeobecné nariadenie o ochrane údajov, článok 4 ods. 11.

368 Tamže, odôvodnenie 42.

Požiadavky na súhlas detí

V GDPR sa stanovuje osobitná ochrana detí v súvislosti s poskytovaním služieb informačnej spoločnosti, pretože „si môžu byť v menšej miere vedomé rizík, dôsledkov a dotknutých záruk a svojich práv súvisiacich so spracúvaním osobných údajov“³⁶⁹. Preto **podľa právnych predpisov EÚ**, ak poskytovatelia služieb informačnej spoločnosti spracúvajú osobné údaje detí vo veku do 16 rokov na základe súhlasu, takéto spracúvanie je zákonné „iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil nositeľ rodičovských práv a povinností“³⁷⁰. Členské štáty môžu vo vnútroštátnych právnych predpisoch stanoviť nižší vek, nesmie však byť nižší ako 13 rokov³⁷¹. Súhlas nositeľa rodičovských práv a povinností nie je potrebný „v súvislosti s preventívnymi alebo poradenskými službami, ktoré sú ponúkané priamo deťom“³⁷². Informácie a komunikácia, v prípade, že sa spracúvanie zameriava na dieťa, by mali byť formulované jasne a jednoducho, aby ich dieťa mohlo ľahko pochopiť³⁷³.

Právo kedykoľvek odvolať súhlas

GDPR obsahuje všeobecné právo kedykoľvek odvolať svoj súhlas³⁷⁴. Dotknutá osoba musí byť informovaná o tomto práve pred poskytnutím súhlasu a toto právo môže uplatniť podľa vlastného uváženia. Nemala by existovať požiadavka uvádzať dôvody odvolania ani žiadne riziko negatívnych dôsledkov nad rámec ukončenia akýchkoľvek výhod, ktoré mohli vyplývať z pôvodne dohodnutého využívania údajov. Odvolanie súhlasu musí byť také jednoduché ako jeho poskytnutie³⁷⁵. Súhlas sa nemôže považovať za slobodný, ak dotknutá osoba nie je schopná svoj súhlas odvolať bez nepriaznivých následkov alebo ak odvolanie súhlasu nie je rovnako jednoduché ako jeho poskytnutie³⁷⁶.

369 Tamže, odôvodnenie 38.

370 Tamže. Článok 8 ods. 1 prvá zarážka. Pojem služby informačnej spoločnosti je vymedzený v článku 4 bode 25 všeobecného nariadenia o ochrane údajov.

371 Všeobecné nariadenie o ochrane údajov, článok 8 ods. 1, druhá zarážka.

372 Tamže, odôvodnenie 38.

373 Tamže, odôvodnenie 58. Pozri aj modernizovaný Dohovor č. 108, článok 15 ods. 2 písm. e). Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 68 a 125.

374 Všeobecné nariadenie o ochrane údajov, článok 7 ods. 3. Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 45.

375 Všeobecné nariadenie o ochrane údajov, článok 7 ods. 3.

376 Všeobecné nariadenie o ochrane údajov, odôvodnenie 42; dôvodová správa k modernizovanému Dohovoru č. 108, bod 42.

Príklad: Zákazník súhlasí so zasielaním reklamných e-mailov na adresu, ktorú poskytol prevádzkovateľovi. Ak zákazník svoj súhlas odvolá, prevádzkovateľ musí ihneď zastaviť zasielanie reklamných e-mailov. Nesmie zákazníkovi ukladať žiadne postihy, napríklad poplatky. Odvolanie však platí do budúcnosti a nemá spätný účinok. Obdobie, počas ktorého sa osobné údaje klienta spracúvali zákonným spôsobom – z dôvodu súhlasu zákazníka – bolo legítimne. Odvolanie bráni akémukoľvek ďalšiemu spracúvaniu týchto údajov, pokiaľ takéto spracúvanie nie je v súlade s právom na výmaz³⁷⁷.

Nevyhnutnosť na plnenie zmluvy

Podľa právnych predpisov EÚ článok 6 ods. 1 písm. b) GDPR poskytuje ďalší základ na legítimne spracúvanie, a to, ak je „nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba“. Toto ustanovenie sa vzťahuje aj na predzmluvné vzťahy. Napríklad v prípadoch, keď má strana v úmysle uzavrieť zmluvu, ale ešte tak neurobila, pravdepodobne z dôvodu, že ešte potrebuje dokončiť overovanie zmluvy. Ak niektorá zo strán potrebuje spracúvať údaje na tento účel, takéto spracúvanie je legítimne, pokiaľ je „nevyhnutné [...] aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy“³⁷⁸.

Pojem spracúvanie údajov ako „legitímny základ stanovený v právnych predpisoch“ v článku 5 ods. 2 modernizovaného Dohovoru č. 108 zahŕňa aj „spracúvanie údajov na účely plnenia zmluvy (alebo vykonanie predzmluvných opatrení na žiadosť dotknutej osoby), ktorej zmluvnou stranou je dotknutá osoba“³⁷⁹.

Zákonné povinnosti prevádzkovateľa

V **právnych predpisoch EÚ** sa stanovuje ďalší dôvod zákonnosti spracúvania, a to v prípade, ak „je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa“ [článok 6 ods. 1 písm. c) GDPR]. Toto ustanovenie sa týka prevádzkovateľov pôsobiach v súkromnom aj vo verejnom sektore; na zákonné povinnosti prevádzkovateľov vo verejnom sektore sa takisto môže vzťahovať článok 6 ods. 1 písm. e) GDPR. Existuje mnoho príkladov situácií, keď zákon ukladá prevádzkovateľom

377 Všeobecné nariadenie o ochrane údajov, článok 17 ods. 1 písm. b).

378 Tamže, článok 6 ods. 1 písm. b).

379 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 46; Rada Európy, Výbor ministrov (2010), Odporúčanie Rec(2010)13 členským štátom o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania, 23. novembra 2010, článok 3.4 písm. b).

v súkromnom sektore povinnosť spracúvať údaje o konkrétnych dotknutých osobách. Zamestnávateľia napríklad musia spracúvať údaje o svojich zamestnancoch na účely sociálneho zabezpečenia a zdaňovania a podniky musia spracúvať údaje o svojich zákazníkoch na daňové účely.

Zákonná povinnosť môže mať pôvod v práve Únie alebo v práve členského štátu, ktoré môže byť základom pre jednu alebo viacero spracovateľských operácií. Na základe tohto práva by sa malo rozhodovať o účele spracúvania, stanoviť špecifikácie na určenie prevádzkovateľa, typu osobných údajov, ktoré podliehajú spracúvaniu, príslušných dotknutých osôb, subjektov, ktorým môžu byť osobné údaje poskytnuté, obmedzenia účelu, obdobia uchovávania a iných opatrení s cieľom zabezpečiť zákonné a spravodlivé spracúvanie³⁸⁰. Každý takýto právny predpis, ktorý je základom na spracúvanie osobných údajov, musí byť v súlade s článkami 7 a 8 Charty a článkom 8 ECHR.

Zákonné povinnosti prevádzkovateľa slúžia aj ako základ na legitímne spracúvanie údajov **podľa právnych predpisov RE**. Ako už bolo uvedené, zákonné povinnosti prevádzkovateľa v súkromnom sektore sú len jedným z konkrétnych prípadov oprávnených záujmov iných, ako sa uvádza v článku 8 ods. 2 ECHR³⁸¹. Príklad zamestnávateľov, ktorí spracúvajú údaje o svojich zamestnancoch, je preto relevantný aj v prípade práva RE.

Životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby

Podľa právnych predpisov EÚ sa v článku 6 ods. 1 písm. d) GDPR stanovuje, že spracúvanie osobných údajov je zákonné, ak je „nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby“. Tento legitímny dôvod sa môže uplatniť len na spracúvanie osobných údajov na základe životne dôležitých záujmov inej fyzickej osoby, ak sa takéto spracúvanie „zjavne nemôže zakladať na inom právnom základe“³⁸². Niekedy môže byť typ spracúvania založený na dôvodoch verejného záujmu, ako aj na dôvodoch životne dôležitých záujmov dotknutej osoby alebo inej osoby. Je to tak napríklad pri monitorovaní epidémií a ich vývoja alebo v prípade núdzovej humanitárnej situácie.

380 Všeobecné nariadenie o ochrane údajov, odôvodnenie 45.

381 Rada Európy, Výbor ministrov (2010), Odporúčanie Rec(2010)13 členským štátom o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania, 23. novembra 2010, článok 3.4 písm. a).

382 Všeobecné nariadenie o ochrane údajov, odôvodnenie 46.

V práve RE sa v článku 8 ECHR životne dôležité záujmy dotknutej osoby neuvádzajú. Životne dôležité záujmy dotknutej osoby sa však považujú za implicitne zahrnuté do pojmu „legitímny základ“ v článku 5 ods. 2 modernizovaného Dohovoru č. 108, ktorý sa zaoberá legitímnosťou spracúvania osobných údajov³⁸³.

Verejný záujem a výkon verejnej moci

Vzhľadom na mnohé možné spôsoby organizácie verejných záležitostí sa v článku 6 ods. 1 písm. e) GDPR stanovuje, že osobné údaje sa môžu zákonne spracúvať, ak to je „nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi [...]“³⁸⁴.

Príklad: Vo veci *Huber/Bundesrepublik Deutschland*³⁸⁵ požiadal pán Huber, rakúsky štátny príslušník s bydliskom v Nemecku, Spolkový úrad pre migráciu a utečencov, aby z centrálného registra zahraničných štátnych príslušníkov („AZR“) odstránil údaje, ktoré sa ho týkajú. Tento register, ktorý obsahuje osobné údaje štátnych príslušníkov iných členských štátov EÚ ako Nemecka bývajúcich v Nemecku dlhšie ako tri mesiace, sa používa na štatistické účely a zo strany orgánov presadzovania práva a súdnych orgánov pri vyšetrovaní a stíhaní páchatelov trestnej činnosti alebo osôb, ktoré ohrozujú verejnú bezpečnosť. Súd, ktorý položil prejudiciálnu otázku, sa pýtal, či je spracúvanie osobných údajov, ku ktorému dochádza v registroch, ako je centrálny register zahraničných štátnych príslušníkov, do ktorého majú prístup aj ďalšie verejné orgány, zlučiteľné s právnymi predpismi EÚ, vzhľadom na to, že neexistuje žiadny podobný register pre nemeckých štátnych príslušníkov.

SDEÚ konštatoval, že podľa článku 7 písm. e) smernice 95/46³⁸⁶ je spracúvanie osobných údajov zákonné len vtedy, keď je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo pri výkone verejnej moci.

383 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 46.

384 Pozri všeobecné nariadenie o ochrane údajov, odôvodnenie 45.

385 SDEÚ, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008.

386 Predtým smernica o ochrane údajov, článok 7 písm. e), teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. e).

Podľa SDEÚ „vzhľadom na cieľ, ktorým je zabezpečenie rovnakej úrovne ochrany vo všetkých členských štátoch, preto nemôže mať pojem nevyhnutnosť, ako vyplýva z článku 7 písm. e) smernice 95/46³⁸⁷ [...] odlišný obsah v jednotlivých členských štátoch. Ide preto o autonómny pojem práva Spoločenstva, ktorý musí byť vykladaný tak, aby plne zodpovedal cieľu tejto smernice, ako je definovaný v jej článku 1 ods. 1“³⁸⁸.

SDEÚ poznamenal, že právo občanov Únie na voľný pohyb na území členského štátu, ktorého daný občan nie je štátnym príslušníkom, nie je nepodmienené a môžu sa naň vzťahovať obmedzenia a podmienky uložené Zmluvou o fungovaní EÚ a opatreniami, ktorých prostredníctvom sa vykonáva. V zásade je každý členský štát oprávnený používať podobný register ako je AZR ako pomôcku pre orgány zodpovedné za uplatňovanie právnych predpisov týkajúcich sa práva na pobyt; register však nesmie obsahovať žiadne iné informácie okrem tých, ktoré sú nevyhnutne potrebné na daný účel. SDEÚ dospel k záveru, že takýto systém spracúvania osobných údajov je v súlade s právnymi predpismi EÚ vtedy, keď obsahuje len údaje nevyhnutné na uplatňovanie daných právnych predpisov a jeho centralizovaná povaha zefektívňuje uplatňovanie príslušnej legislatívy. V tomto konkrétnom prípade musí splnenie uvedených požiadaviek posúdiť vnútroštátny súd. Ak by podmienky neboli splnené, uchovávanie a spracúvanie osobných údajov v registri ako AZR na štatistické účely nemožno v žiadnom prípade pokladať za nevyhnutné v zmysle článku 7 písm. e) ³⁸⁹smernice 95/46/ES³⁹⁰.

Pokiaľ ide o otázku používania údajov obsiahnutých v registri na účely boja proti trestnej činnosti, SDEÚ uvádza, že tento cieľ nevyhnutne zahŕňa „stíhanie spáchaných trestných činov a priestupkov bez ohľadu na štátnu príslušnosť ich páchatelov“. Predmetný register neobsahuje osobné údaje týkajúce sa štátnych príslušníkov dotknutého členského štátu a toto rozdielne zaobchádzanie predstavuje diskrimináciu zakázanú článkom 18 ZFEÚ. Z toho vyplýva, že vo výklade SDEÚ toto ustanovenie „bráni tomu, aby členský

387 Tamže.

388 SDEÚ, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008, bod 52.

389 Predtým smernica o ochrane údajov, článok 7 písm. e), teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. e).

390 SDEÚ, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008, body 54, 58 – 59 a 66 – 68.

štát s cieľom boja proti trestnej činnosti zaviedol systém spracovávania osobných údajov týkajúcich sa len občanov Únie, ktorí nie sú jeho štátnymi príslušníkmi³⁹¹.

Na používanie osobných údajov orgánmi konajúcimi vo verejnej sfére sa vzťahuje aj článok 8 **ECHR** a v prípade potreby aj článok 5 ods. 2 modernizovaného Dohovoru č. 108³⁹².

Oprávnené záujmy, ktoré sleduje prevádzkovateľ alebo tretia strana

Podľa **právnych predpisov EÚ** nie je dotknutá osoba jediným subjektom, ktorý má oprávnené záujmy. V článku 6 ods. 1 písm. f) GDPR sa stanovuje, že osobné údaje sa môžu zákonne spracúvať, ak to „je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana [ktorým sa údaje poskytujú] [okrem orgánov verejnej moci pri výkone ich úloh], s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu [...]“³⁹³.

Existencia oprávneného záujmu sa musí dôkladne posúdiť v každom konkrétnom prípade³⁹⁴. Ak existujú oprávnené záujmy prevádzkovateľa, musia sa vyvážiť voči záujmom alebo základným právam a slobodám dotknutej osoby³⁹⁵. Pri takomto vyvážení sa musí zohľadniť primerané očakávanie dotknutej osoby, aby sa zistilo, či záujmy prevádzkovateľa prevažujú nad záujmami alebo základnými právami dotknutej osoby³⁹⁶. Ak práva dotknutej osoby prevažujú nad oprávnenými záujmami prevádzkovateľa, prevádzkovateľ môže prijať opatrenia a zaviesť záruky na zabezpečenie toho, aby sa vplyv na práva dotknutej osoby minimalizoval (napríklad pseudonymizácia), a zmeniť rovnováhu pred tým, než sa zákonne spoľahne na tento legitímny základ na spracúvanie. Pracovná skupina zriadená podľa článku 29 vo svojom stanovisku k pojmu legitímne (oprávnené) záujmy prevádzkovateľa zdôraznila kľúčovú úlohu zodpovednosti a transparentnosti, ako aj práv dotknutej osoby namietat'

391 Tamže, body 78 a 81.

392 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 46 a 47.

393 V porovnaní so smernicou 95/46 poskytuje všeobecné nariadenie o ochrane údajov viac príkladov prípadov, ktoré sa považujú za oprávnený záujem.

394 Všeobecné nariadenie o ochrane údajov, preambula, odôvodnenie 47.

395 Pracovná skupina zriadená podľa článku 29 (2014) *Stanovisko 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES*, 4. apríla 2014.

396 Tamže.

proti spracúvaniu jej údajov alebo prístupu k nim, ich zmene, vymazaniu alebo presunu, pri zväžení oprávnených záujmov prevádzkovateľa a záujmov základných práv dotknutej osoby³⁹⁷.

V odôvodneniach GDPR sa uvádza niekoľko príkladov toho, čo predstavuje oprávnený záujem dotknutého prevádzkovateľa. Spracúvanie osobných údajov sa napríklad povoľuje bez súhlasu dotknutej osoby, ak sa vykonáva na účely priameho marketingu alebo ak je takéto spracúvanie „nevyhnutne potrebné na účely predchádzania podvodom“³⁹⁸.

SDEÚ vo svojej judikatúre rozšíril kritéria určovania oprávneného záujmu.

Príklad: Vo veci *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*³⁹⁹ išlo o poškodenie trolejbusu spoločnosti Rīgas Transport Company, ku ktorému došlo, keď cestujúci náhle otvoril dvere taxíka. Spoločnosť Rīgas satiksme chcela cestujúceho žalovať o náhradu škody. Polícia však poskytla len meno cestujúceho a odmietla poskytnúť identifikačné číslo a adresu cestujúceho s odôvodnením, že ich poskytnutie by bolo podľa vnútroštátnych zákonov o ochrane údajov nezákonné.

Lotyšský vnútroštátny súd požiadal SDEÚ o prejudiciálne rozhodnutie o tom, či právne predpisy EÚ o ochrane údajov ukladajú povinnosť oznámiť všetky osobné údaje potrebné na začatie občianskoprávneho konania proti osobe, ktorá je údajne zodpovedná za priestupok⁴⁰⁰.

SDEÚ objasnil, že právo EÚ v oblasti ochrany údajov zahŕňa možnosť – nie povinnosť – poskytnúť údaje tretej strane na účely oprávnených záujmov, ktoré táto strana sleduje⁴⁰¹. SDEÚ stanovil tri kumulatívne podmienky, ktoré musia byť splnené na to, aby bolo spracúvanie osobných údajov zákonné na základe „oprávnených záujmov“⁴⁰². Po prvé musí tretia strana, ktorej sú údaje sprístupnené, sledovať oprávnený záujem. V tomto konkrétnom

397 Tamže.

398 Všeobecné nariadenie o ochrane údajov, preambula, odôvodnenie 47.

399 SDEÚ, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA "Rīgas satiksme"*, 4. mája 2017.

400 Tamže, bod 23.

401 Tamže, bod 26.

402 Tamže, body 28 – 34.

případe to znamená, že žiadosť o osobné informácie na účel podania žaloby o náhradu škody na majetku predstavuje oprávnený záujem tretej strany. Po druhé musí byť spracúvanie osobných údajov nevyhnutné na účely sledovaného oprávneného záujmu. V tomto prípade je na zistenie totožnosti osoby nevyhnutné získať osobné informácie, ako je adresa a/alebo identifikačné číslo. Po tretie nesmú mať základné práva a slobody dotknutej osoby prednosť pred oprávnenými záujmami prevádzkovateľa alebo tretej osoby. Záujmy sa musia vyvažovať v každom jednotlivom prípade pri zohľadnení okolností, ako je závažnosť porušenia práv dotknutej osoby alebo za určitých okolností aj vek dotknutej osoby. V tomto konkrétnom prípade však SDEÚ nepovažoval zamietnutie poskytnutia za opodstatnené, keďže dotknutá osoba bola maloletá.

V rozsudku vo veci *ASNEF a FECEMD* SDEÚ výslovne rozhodol o spracúvaní údajov na základe právneho základu „oprávneného záujmu“, ktorý bol v tom čase zakotvený v článku 7 písm. f) smernice o ochrane údajov⁴⁰³.

Príklad: SDEÚ vo veci *ASNEF a FECEMD*⁴⁰⁴ vysvetlil, že vo vnútroštátnych právnych predpisoch sa nemôžu pridávať podmienky okrem tých, ktoré sú uvedené v článku 7 písm. f) smernice, pokiaľ ide o zákonné spracúvanie údajov⁴⁰⁵. Týkalo sa to situácie, keď španielsky právny predpis o ochrane údajov obsahoval ustanovenie, podľa ktorého by iné súkromné strany mohli mať oprávnený záujem na spracúvaní osobných údajov len vtedy, keď informácie predtým figurovali vo verejne prístupných zdrojoch.

SDEÚ najprv uviedol, že účelom smernice 95/46⁴⁰⁶ je zaistiť rovnocennosť úrovne ochrany práv a slobôd jednotlivcov v súvislosti so spracúvaním osobných údajov vo všetkých členských štátoch. Ani aproximácia vnútroštátnych právnych predpisov v tejto oblasti nesmie viesť k zníženiu stupňa poskytovanej ochrany. Naopak, jej cieľom musí byť zaistenie vysokej úrovne ochrany

403 Predtým smernica o ochrane údajov, článok 7 písm. f), teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. f).

404 SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24. novembra 2011.

405 Predtým smernica o ochrane údajov, článok 7 písm. f), teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. f).

406 Predtým smernica o ochrane údajov, teraz všeobecné nariadenie o ochrane údajov.

v EÚ⁴⁰⁷. Následne SDEÚ konštatoval, že „z cieľa spočívajúceho v zabezpečení rovnakej úrovne ochrany vo všetkých členských štátoch vyplýva, že článok 7 smernice 95/46⁴⁰⁸ stanovuje taxatívny zoznam prípadov, v ktorých možno spracúvanie osobných údajov považovať za prípustné“. Okrem toho „členské štáty nemôžu ani pridať nové zásady týkajúce sa zákonnosti spracovania osobných údajov do článku 7 smernice 95/46⁴⁰⁹, ani stanoviť dodatočné požiadavky, ktoré by menili rozsah jednej zo [šiestich] zásad stanovených“ v článku 7⁴¹⁰. SDEÚ pripustil, že, pokiaľ ide o zväzanie potrebné podľa článku 7 písm. f) smernice 95/46, je možné zohľadniť, že závažnosť porušenia základných práv osoby dotknutej týmto spracúvaním sa môže odlišovať v závislosti od toho, či predmetné údaje už figurujú alebo ešte nefigurujú vo verejne prístupných zdrojoch.

Článok 7 písm. f) tejto smernice však „odporuje tomu, aby členský štát kategoricky a všeobecne vylúčil možnosť spracovať určité kategórie osobných údajov bez toho, aby pripustil zvážiť protichodné práva a záujmy, o ktoré ide v konkrétnom prípade“.

Vzhľadom na uvedené skutočnosti SDEÚ dospel k záveru, že článok 7 písm. f) smernice 95/46⁴¹¹ sa má vykladať v tom zmysle, „že mu odporuje vnútroštátna právna úprava, ktorá pri absencii súhlasu zo strany dotknutej osoby a na povolenie spracovania osobných údajov o nej, ktoré je potrebné na splnenie legitímneho záujmu, ktorý sleduje osoba zodpovedná za spracovanie alebo tretie osoby, ktorým sa údaje oznamujú, vyžaduje popri dodržiavaní základných práv a slobôd dotknutej osoby, aby sa predmetné údaje nachádzali vo verejne prístupných zdrojoch, kategoricky a všeobecne tak vylučujúc akékoľvek spracovávanie údajov, ktoré nie sú uvedené v takýchto verejne prístupných zdrojoch“⁴¹².

407 SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECMD)/Administración del Estado*, 24. novembra 2011, bod 28. Pozri smernicu o ochrane údajov, odôvodnenia 8 a 10.

408 Predtým smernica o ochrane údajov, článok 7, teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. f).

409 Predtým smernica o ochrane údajov, článok 7, teraz všeobecné nariadenie o ochrane údajov, článok 6.

410 Tamže.

411 Predtým smernica o ochrane údajov, článok 7 písm. f), teraz všeobecné nariadenie o ochrane údajov, článok 6 ods. 1 písm. f).

412 SDEÚ, spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECMD)/Administración del Estado*, 24. novembra 2011, body 40, 44 a 48 – 49.

Vždy, keď sa osobné údaje spracúvajú na základe „oprávnených záujmov“, má jednotlivec právo kedykoľvek namietat' proti spracúvaniu z dôvodov súvisiacich s jeho konkrétnou situáciou podľa článku 21 ods. 1 GDPR. Prevádzkovateľ musí zastaviť spracúvanie, pokiaľ nepreukáže nevyhnutné legitímne dôvody na jeho pokračovanie.

Pokiaľ ide o **právne predpisy RE**, podobné formulácie možno nájsť v modernizovanom Dohovore č. 108⁴¹³ a odporúčaní RE. V odporúčaní o profilovaní sa uznáva spracúvanie osobných údajov na účely profilovania ako legitímne, ak je potrebné pre oprávnené záujmy ostatných, „s výnimkou prípadov, keď nad takýmito záujmami prevažujú základné práva a slobody dotknutých osôb“⁴¹⁴. Okrem toho, „ochrana práv a slobôd iných“ sa v článku 8 ods. 2 ECHR uvádza ako jeden z legitímnych dôvodov na obmedzenie práva na ochranu údajov.

Príklad: Vo veci *Y/Turecko*⁴¹⁵ bol sťažovateľ HIV pozitívny. Keďže bol počas svojho príchodu do nemocnice v bezvedomí, posádka sanitky informovala pracovníkov nemocnice, že je HIV pozitívny. Sťažovateľ pred ESLP tvrdil, že zverejnenie týchto informácií porušilo jeho právo na rešpektovanie súkromného života. Vzhľadom na potrebu zaručiť bezpečnosť zamestnancov nemocnice sa však poskytnutie tejto informácie nepovažovalo za porušenie jeho práv.

4.1.2. Spracúvanie osobitných kategórií údajov (citlivých údajov)

Právne predpisy RE stanovenie primeranej ochrany pri zaobchádzaní s citlivými údajmi ponechávajú na vnútroštátnych právnych predpisoch za predpokladu, že sú splnené podmienky článku 6 modernizovaného Dohovoru č. 108, konkrétne, že primerané záruky, ktoré dopĺňajú ostatné ustanovenia Dohovoru, sú zakotvené v právnych predpisoch. **V právnych predpisoch EÚ** sa v článku 9 GDPR uvádza podrobný režim spracúvania osobitných kategórií údajov (tzv. „citlivých údajov“). Tieto údaje odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické

⁴¹³ Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 46.

⁴¹⁴ Rada Európy, Výbor ministrov (2010), *Odporúčanie Rec(2010)13 členským štátom a dôvodová správa o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania*, 23. novembra 2010, článok 3.4 písm. b) (odporúčanie o profilovaní).

⁴¹⁵ ESLP, *Y/Turecko*, č. 648/10, 17. februára 2015.

presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby. Spracúvanie citlivých údajov je v zásade zakázané⁴¹⁶.

Existuje však taxatívny zoznam výnimiek z tohto zákazu, ktoré možno nájsť v článku 9 ods. 2 tohto nariadenia a ktoré predstavujú právne základy na spracúvanie citlivých údajov. Tieto výnimky zahŕňajú situácie, keď:

- dotknutá osoba vyjadrila výslovný súhlas so spracúvaním údajov,
- spracúvanie vykonáva v rámci svojej zákonnej činnosti neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi,
- spracúvanie sa týka údajov, ktoré dotknutá osoba výslovne zverejnila,
- spracúvanie je nevyhnutné:
 - na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany,
 - na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je schopná vyjadriť svoj súhlas,
 - na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc,
 - na účely preventívneho alebo pracovného lekárstva: „posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom“,

⁴¹⁶ Predtým smernica o ochrane údajov, článok 7 písm. f), teraz všeobecné nariadenie o ochrane údajov, článok 9 ods. 1.

- na účely archivácie vo verejnom záujme alebo na účely vedeckého alebo historického výskumu, či na štatistické účely.
- z dôvodov verejného záujmu v oblasti verejného zdravia, alebo
- z dôvodov významného verejného záujmu.

Pri spracúvaní osobitných kategórií údajov sa zmluvný vzťah s dotknutou osobou preto nepovažuje za právny základ na legitímne spracúvanie citlivých údajov, s výnimkou zmluvy so zdravotníckym pracovníkom, na ktorého sa vzťahuje povinnosť zachovávať služobné tajomstvo⁴¹⁷.

Výslovný súhlas dotknutej osoby

Podľa **právnych predpisov EÚ** je prvou podmienkou zákonného spracúvania akýchkoľvek údajov bez ohľadu na to, či sú alebo nie sú citlivé, súhlas dotknutej osoby. V prípade citlivých údajov musí byť tento súhlas výslovný. V právnych predpisoch Únie alebo členského štátu sa však môžu stanovovať, že jednotlivец nemôže zrušiť zákaz spracúvania osobitných kategórií údajov⁴¹⁸. Môže ísť napríklad o prípad, keď spracúvanie zahŕňa nezvyčajné riziká pre dotknutú osobu.

Pracovné právo alebo právne predpisy v oblasti sociálneho zabezpečenia a sociálnej ochrany

Podľa **právnych predpisov EÚ** možno zákaz uvedený v článku 9 ods. 1 zrušiť, ak je spracúvanie potrebné na plnenie povinností alebo práv prevádzkovateľa alebo dotknutej osoby v oblasti zamestnanosti alebo sociálneho zabezpečenia. Spracúvanie však musí byť povolené právom EÚ, vnútroštátnym právom alebo kolektívnou zmluvou podľa vnútroštátneho práva, ktoré poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby⁴¹⁹. Záznamy o zamestnaní, ktoré vedie organizácia, môžu za určitých podmienok uvedených v GDPR a v príslušnom vnútroštátnom práve zahŕňať citlivé osobné údaje. Príkladmi citlivých údajov môžu byť členstvo v odborových organizáciách alebo informácie o zdraví.

417 Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. h) a i).

418 Tamže, článok 9 ods. 2 písm. a).

419 Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. b).

Životne dôležité záujmy dotknutej osoby alebo inej osoby

Podľa právnych predpisov EÚ sa citlivé údaje, rovnako ako údaje, ktoré nie sú citlivé, môžu spracúvať z dôvodu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby⁴²⁰. Ak je spracúvanie založené na životne dôležitých záujmoch inej osoby, tento legitímny dôvod sa môže uplatniť, len ak sa takéto spracúvanie „zjavne nemôže zakladať na inom právnom základe“⁴²¹. V niektorých prípadoch môže spracúvanie osobných údajov chrániť tak záujmy jednotlivcov, ako aj verejné záujmy, napríklad keď je spracúvanie nevyhnutné na humanitárne účely⁴²².

Aby bolo spracúvanie citlivých údajov legitímne na tomto základe, muselo by byť nemožné požiadať dotknutú osobu o súhlas, pretože napríklad bola v bezvedomí alebo nebola prítomná a nebolo možné sa s ňou skontaktovať. Inými slovami, osoba bola fyzicky alebo právne nespôsobilá vyjadriť súhlas.

Charity alebo neziskové subjekty

Spracúvanie osobných údajov je povolené aj v rámci zákonných činností nadácií, združení alebo iných neziskových subjektov s politickým, filozofickým, náboženským alebo odborárskym zameraním. Spracúvanie sa však musí týkať výlučne členov alebo bývalých členov, alebo osôb, ktoré majú pravidelný kontakt s týmto subjektom⁴²³. Citlivé údaje nemožno poskytovať mimo týchto subjektov bez súhlasu dotknutej osoby.

Údaje preukázateľne zverejnené dotknutou osobou

V článku 9 ods. 2 písm. e) GDPR sa stanovuje, že spracúvanie nie je zakázané, ak sa týka údajov, ktoré dotknutá osoba preukázateľne zverejnila. Aj keď význam formulácie „ktoré dotknutá osoba preukázateľne zverejnila“ nie je v nariadení vymedzený, keďže ide o výnimku zo zákazu spracúvania citlivých údajov, musí sa vykladať striktno a v tom zmysle, že sa od dotknutej osoby vyžaduje, aby svoje osobné údaje zverejnila úmyselne. Preto v prípade, že v televíznom vysielaní je odvysielaný videozáznam z kamerového monitorovacieho systému, na ktorom okrem iného vidno hasiča, ktorý sa zraní pri evakuácii budovy, nemožno sa domnievať, že tento hasič

420 Tamže, článok 9 ods. 2 písm. c).

421 Tamže, odôvodnenie 46.

422 Tamže.

423 Tamže, článok 9 ods. 2 písm. d).

preukázateľne zverejnil údaje. Na druhej strane, ak sa hasič rozhodne opísať túto udalosť a zverejniť videozáznam a fotografie na verejnej internetovej stránke, predstavovalo by to úmyselný prejav vôle s cieľom zverejniť osobné údaje. Je dôležité poznamenať, že zverejnenie osobných údajov nepredstavuje súhlas, ale iné povolenie na spracúvanie osobitných kategórií údajov.

Skutočnosť, že dotknutá osoba zverejnila spracúvané osobné údaje, nezavaruje prevádzkovateľov povinností, ktoré im vyplývajú z právnych predpisov o ochrane údajov. Nadalej sa napríklad na tieto osobné údaje uplatňuje zásada obmedzenia účelu, aj keď boli sprístupnené verejnosti⁴²⁴.

Právne nároky

Spracúvanie osobitných kategórií údajov, ktoré „je potrebné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, a to bez ohľadu na to, či ide súdne alebo správne konanie alebo mimosúdne konanie“⁴²⁵, je povolené aj podľa GDPR⁴²⁶. V tomto prípade sa spracúvanie musí týkať konkrétneho právneho nároku a jeho uplatnenia alebo obhajoby a môže ho požadovať ktorýkoľvek účastník sporu.

Keď súdy vykonávajú svoju súdnu právomoc, môžu spracúvať osobitné kategórie údajov v rámci riešenia právneho sporu⁴²⁷. Príklady týchto osobitných kategórií údajov spracúvaných v tejto súvislosti by mohli zahŕňať napríklad genetické údaje pri určovaní rodičovstva alebo zdravotný stav, ak sa časť dôkazov týka podrobností o zranení, ktoré utrpela obeť trestného činu.

Dôvody významného verejného záujmu

Podľa článku 9 ods. 2 písm. g) GDPR môžu členské štáty určiť ďalšie okolnosti, za ktorých sa citlivé údaje môžu spracúvať, pokiaľ:

- spracúvanie údajov je nevyhnutné z dôvodov významného verejného záujmu,

424 Pracovná skupina zriadená podľa článku 29 (2013), *Stanovisko 3/13 k obmedzeniu účelu*, WP 203, Brusel, 2. apríla 2013, s. 14.

425 Všeobecné nariadenie o ochrane údajov, preambula, odôvodnenie 52.

426 Tamže, článok 9 ods. 2 písm. f).

427 Tamže.

- to je na základe právnych predpisov Únie alebo vnútroštátnych právnych predpisov,
- právne predpisy Únie alebo vnútroštátne právne predpisy sú primerané, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie práv a záujmov dotknutej osoby⁴²⁸.

Významným príkladom sú systémy elektronických zdravotných záznamov. Tieto systémy umožňujú, aby sa údaje týkajúce sa zdravia, ktoré získali poskytovatelia zdravotnej starostlivosti počas starostlivosti o pacienta, sprístupnili iným poskytovateľom zdravotnej starostlivosti tohto pacienta, a to vo veľkom rozsahu a obvykle celoštátne.

Pracovná skupina zriadená podľa článku 29 dospela k záveru, že takéto systémy by sa podľa platných právnych predpisov o spracúvaní údajov o pacientoch nemohli vytvárať⁴²⁹. Existencia takýchto systémov elektronických zdravotných záznamov je však možná, ak sú založené na „[dôvodoch] významného verejného záujmu“⁴³⁰. Vyžaduje si to výslovný právny základ na ich zriadenie, ktorý by obsahoval aj potrebné záruky, aby sa zabezpečilo, že systém bude fungovať bezpečne⁴³¹.

Iné dôvody na spracúvanie citlivých údajov

V GDPR sa stanovuje, že citlivé údaje možno spracúvať, ak je spracúvanie nevyhnutné⁴³²:

- na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva Únie alebo práva členského štátu alebo podľa zmluvy so zdravotníckym pracovníkom,

428 Tamže, článok 9 ods. 2 písm. g).

429 Pracovná skupina zriadená podľa článku 29 (2007), *pracovný dokument o spracovaní osobných údajov týkajúcich sa zdravotného stavu v elektronických zdravotných záznamoch (EZZ)*, WP 131, Brusel, 15. februára 2007. Pozri aj všeobecné nariadenie o ochrane údajov, článok 9 ods. 3.

430 Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. g).

431 Pracovná skupina zriadená podľa článku 29 (2007), *pracovný dokument o spracovaní osobných údajov týkajúcich sa zdravotného stavu v elektronických zdravotných záznamoch (EZZ)*, WP 131, Brusel, 15. februára 2007.

432 Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. h), i) a j).

- z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok, na základe práva Únie alebo práva členského štátu. V príslušnom práve sa musia stanovovať vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby,
- na účely archivácie vo verejnom záujme, alebo na účely vedeckého alebo historického výskumu či na štatistické účely na základe práva Únie alebo práva členského štátu. Právne predpisy musia byť primerané vzhľadom na sledovaný cieľ, rešpektovať podstatu práva na ochranu údajov a určovať vhodné a konkrétne opatrenia na zabezpečenie práv a záujmov dotknutej osoby.

Dodatočné podmienky podľa vnútroštátneho práva

Podľa GDPR sa členským štátom takisto umožňuje zaviesť alebo zachovať dodatočné podmienky vrátane obmedzení týkajúcich sa spracúvania genetických, biometrických a zdravotných údajov⁴³³.

4.2. Pravidlá bezpečnosti spracúvania

Hlavné body

- Pravidlá v oblasti bezpečnosti spracúvania zaväzujú prevádzkovateľa a sprostredkovateľa, aby prijali primerané technické a organizačné opatrenia s cieľom predísť akémukoľvek neoprávnenému zasahovaniu do spracovateľských operácií.
- Nevyhnutná úroveň bezpečnosti osobných údajov je určená:
 - bezpečnostnými prvkami dostupnými na trhu pre konkrétny typ spracúvania,
 - nákladmi,
 - rizikami spracúvania údajov pre základné práva a slobody dotknutých osôb.
- Zabezpečenie dôvernosti osobných údajov je súčasťou všeobecnej zásady uznanej vo všeobecnom nariadení o ochrane údajov.

⁴³³ Tamže, článok 9 ods. 2 písm. h) a článok 9 ods. 4.

Podľa **právnych predpisov EÚ, ako aj RE** majú prevádzkovatelia všeobecnú povinnosť byť pri spracúvaní osobných údajov transparentní a zodpovední, a to najmä v prípade porušenia ochrany údajov, ak k nemu dôjde. Porušenie ochrany osobných údajov musia prevádzkovatelia oznámiť dozorným orgánom, s výnimkou prípadov, keď je nepravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. O porušení ochrany osobných údajov by mali byť informované aj dotknuté osoby, ak je pravdepodobné, že povedie k vysokému riziku pre práva a slobody fyzických osôb.

4.2.1. Prvky bezpečnosti údajov

Podľa príslušných ustanovení **právnych predpisov EÚ**:

„Prevádzkovateľ a sprostredkovateľ prijímú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku [...]“⁴³⁴.

Medzi tieto opatrenia patria okrem iného:

- pseudonymizácia a šifrovanie osobných údajov⁴³⁵,
- zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania a služieb⁴³⁶,
- včasné obnovenie dostupnosti osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu⁴³⁷,
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania⁴³⁸.

⁴³⁴ Tamže, článok 32 ods. 1.

⁴³⁵ Tamže, článok 32 ods. 1 písm. a).

⁴³⁶ Tamže, článok 32 ods. 1 písm. b).

⁴³⁷ Tamže, článok 32 ods. 1 písm. c).

⁴³⁸ Tamže, článok 32 ods. 1 písm. d).

V **právnych predpisoch RE** existuje podobné ustanovenie:

„Každá strana stanoví, že prevádzkovateľ a prípadne sprostredkovateľ prijímú primerané bezpečnostné opatrenia proti rizikám, ako je napríklad náhodný alebo neoprávnený prístup, zničenie, strata, používanie, zmena alebo zverejnenie osobných údajov“⁴³⁹.

Podľa **právnych predpisov EÚ a RE** je pri porušení údajov, ktoré môže mať vplyv na práva a slobody fyzických osôb, prevádzkovateľ povinný oznámiť porušenie dozornému orgánu (pozri [oddiel 4.2.3](#)).

Často existujú priemyselné, vnútroštátne a medzinárodné normy, ktoré sú určené na zaistenie bezpečnosti spracúvania osobných údajov. Ide napríklad o projekt európskeho osvedčenia o zachovaní dôverného charakteru informácií – European Privacy Seal (EuroPriSe) v rámci európskeho programu podpory transeurópskych telekomunikačných sietí (eTEN), skúmajúci možnosti certifikácie produktov, predovšetkým softvéru, ktoré uľahčujú dodržiavanie európskych právnych predpisov o ochrane údajov. Bola zriadená Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), ktorá má zvýšiť schopnosť EÚ, členských štátov EÚ a podnikateľskej komunity predchádzať problémom s bezpečnosťou sietí a informácií, riešiť ich a reagovať na ne⁴⁴⁰. Agentúra ENISA pravidelne zverejňuje analýzy aktuálnych bezpečnostných hrozieb a radí, ako na ne reagovať⁴⁴¹.

Bezpečnosť osobných údajov sa nedosiahne len inštaláciou správneho vybavenia – hardvéru a softvéru. Vyžaduje si takisto primerané vnútorné organizačné pravidlá. V ideálnom prípade by mali zahŕňať tieto okruhy:

- pravidelné informovanie všetkých zamestnancov o pravidlách bezpečnosti údajov a ich povinnostiach vyplývajúcich z právnych predpisov o ochrane údajov, predovšetkým pokiaľ ide o povinnosti týkajúce sa dôvernosti,

⁴³⁹ Modernizovaný Dohovor č. 108, článok 7 ods. 1.

⁴⁴⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004, Ú. v. EÚ L 165, 2013.

⁴⁴¹ Napríklad, ENISA, (2016), *Cyber Security and Resilience of smart cars. Good practices and recommendations*; ENISA (2016), *Security of Mobile Payments and Digital Wallets*.

- jasné rozdelenie povinností a zreteľné vymedzenie kompetencií v otázkach spracúvania údajov, najmä pokiaľ ide o rozhodnutia spracúvať osobné údaje a prenášať údaje tretím stranám,
- použitie osobných údajov len v súlade s pokynmi oprávnenej osoby alebo podľa všeobecne stanovených pravidiel,
- ochrana prístupu do priestorov a k hardvéru a softvéru prevádzkovateľa alebo sprostredkovateľa vrátane kontrol povolení na prístup,
- zaistenie toho, aby povolenia na prístup k osobným údajom udeľovala oprávnená osoba a aby bolo potrebné predloženie príslušných dokladov,
- automatizované protokoly elektronického prístupu k osobným údajom a pravidelné kontroly takýchto protokolov interným dozorným oddelením (čo si vyžaduje zaznamenávanie všetkých spracovateľských činností údajov),
- dôkladné zdokumentovanie iných foriem zverejnenia než automatický prístup k údajom s cieľom preukázať, že nedošlo k žiadnemu nezákonnému poskytnutiu údajov.

Dôležitou súčasťou účinných predbežných bezpečnostných opatrení je ponuka primeranej odbornej prípravy a vzdelávania zamestnancov v oblasti bezpečnosti osobných údajov. Takisto je nutné zaviesť postupy overovania s cieľom zaistiť, aby primerané opatrenia neexistovali len na papieri, ale aby sa aj realizovali a fungovali v praxi (napríklad externé a interné audity).

Opatrenia na zlepšenie úrovne bezpečnosti prevádzkovateľa a sprostredkovateľa zahŕňajú také nástroje, ako sú zodpovedné osoby za ochranu údajov, vzdelávanie zamestnancov v oblasti bezpečnosti, pravidelné audity, penetračné testovanie a pečate kvality.

Príklad: Sťažovateľka vo veci *I/Fínsko*⁴⁴² nebola schopná dokázať, že jej zdravotné záznamy boli nezákonne sprístupnené ďalším zamestnancom nemocnice, v ktorej pracovala. Vnútroštátne súdy preto zamietli jej sťažnosť na porušenie práva na ochranu údajov. ESĽP dospel k záveru, že došlo

442 ESĽP, *I/Fínsko*, č. 20511/03, 17. júla 2008.

k porušeniu článku 8 ECHR, keďže systém registrácie zdravotných záznamov v nemocnici „bol taký, že nebolo možné spätne vyjasniť používanie záznamov o pacientoch, keďže v systéme sa zobrazovalo len päť posledných nahliadnutí a tieto informácie boli odstránené po vrátení spisu do archívu“. Pre súd bolo rozhodujúce, že systém zavedený v nemocnici zjavne nebol v súlade s právnymi požiadavkami obsiahnutými vo vnútroštátnych právnych predpisoch, a vnútroštátne súdy túto skutočnosť náležite nezohľadnili.

EÚ zaviedla smernicu o sieťovej a informačnej bezpečnosti (smernica NIS)⁴⁴³, ktorá je prvým právnym nástrojom EÚ v oblasti kybernetickej bezpečnosti. Cieľom smernice je na jednej strane zlepšiť kybernetickú bezpečnosť na vnútroštátnej úrovni a na strane druhej zvýšiť úroveň spolupráce v rámci EÚ. Stanovujú sa v nej aj povinnosti prevádzkovateľov základných služieb (vrátane prevádzkovateľov v odvetviach energetiky, zdravotníctva, bankovníctva, dopravy, digitálnej infraštruktúry atď.) a poskytovateľov digitálnych služieb s cieľom riadiť riziká, zaistiť bezpečnosť ich sietí a informačných systémov a oznamovať bezpečnostné incidenty.

Výhľad

V septembri 2017 Európska komisia predložila návrh nariadenia zameraný na reformu mandátu agentúry ENISA s cieľom zohľadniť nové právomoci a povinnosti tejto agentúry podľa smernice NIS. Cieľom navrhovaného nariadenia je rozvíjať úlohy agentúry ENISA a posilniť jej úlohu ako „referenčného bodu v ekosystéme kybernetickej bezpečnosti EÚ“⁴⁴⁴. Navrhovaným nariadením by nemali byť dotknuté zásady GDPR a mali by sa objasniť potrebné prvky, ktoré tvoria európske systémy certifikácie kybernetickej bezpečnosti, a zároveň by sa mala posilniť bezpečnosť osobných údajov. Európska komisia zároveň v septembri 2017 predložila návrh vykonávacieho nariadenia, v ktorom sa špecifikujú prvky, ktoré poskytovatelia digitálnych služieb zohľadnia pri zabezpečovaní bezpečnosti ich sietí a informačných systémov, ako sa vyžaduje v článku 16 ods. 8 smernice NIS. V čase prípravy príručky prebiehali rokovania o týchto dvoch návrhoch.

443 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, Ú. v. EÚ L 194, 2016.

444 *Návrh* nariadenia Európskeho parlamentu a Rady o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (akt o kybernetickej bezpečnosti), COM(2017)477, 13. septembra 2017, s. 6.

4.2.2. Dôvernosť

Podľa právnych predpisov EÚ sa v GDPR uznáva dôvernosť osobných údajov ako súčasť všeobecnej zásady⁴⁴⁵. Poskytovatelia verejne dostupných elektronických komunikačných služieb musia zabezpečiť dôvernosť. Majú tiež povinnosť zaručiť bezpečnosť svojich služieb⁴⁴⁶.

Príklad: Zamestnankyňa poisťovacej spoločnosti telefonuje na pracovisku s osobou, ktorá tvrdí, že je klientom poisťovne, a požaduje informácie týkajúce sa príslušnej poisťnej zmluvy.

Povinnosť zachovať dôvernosť údajov klienta si vyžaduje, aby zamestnankyňa uplatnila aspoň minimálne bezpečnostné opatrenia pred zverejnením osobných údajov. Napríklad môže volajúcemu ponúknuť, že zatelefonuje späť na číslo uvedené v spise daného klienta.

Podľa článku 5 ods. 1 písm. f) osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávněným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).

Podľa článku 32 prevádzkovateľ a sprostredkovateľ musia prijať technické a organizačné opatrenia na zabezpečenie vysokej úrovne bezpečnosti. Takéto opatrenia zahŕňajú okrem iného aj pseudonymizáciu a šifrovanie osobných údajov; schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť spracúvania; testovanie a hodnotenie účinnosti opatrení; a schopnosť obnoviť spracúvanie v prípade fyzického alebo technického incidentu. Okrem toho sa dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu môže použiť ako prvok na preukázanie súladu so zásadou integrity a dôvernosti. Navyše, podľa článku 28 GDPR sa v zmluve, ktorá zaväzuje prevádzkovateľa voči sprostredkovateľovi, musí stanoviť, že sprostredkovateľ zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovávajú dôvernosť informácií, alebo aby boli viazané vhodnou zákonnou povinnosťou zachovávať dôvernosť informácií.

⁴⁴⁵ Všeobecné nariadenie o ochrane údajov, článok 5 ods. 1 písm. f).

⁴⁴⁶ Smernica o súkromí a elektronických komunikáciách, článok 5 ods. 1.

Povinnosť zachovávať dôvernosť sa netýka situácií, keď sa osoba údaje nedozvedela ako zamestnanec prevádzkovateľa alebo sprostredkovateľa, ale sama ako súkromná osoba. V tomto prípade sa neuplatňujú články 32 a 28 GDPR, keďže použitie osobných údajov súkromnými osobami je úplne vyňaté z rozsahu pôsobnosti nariadenia a patrí do rámca tzv. výnimky pre domáce činnosti⁴⁴⁷. Výnimkou pre domácu činnosť sa rozumie používanie osobných údajov „fyzickou osobou v priebehu výlučne osobnej alebo domácej činnosti“⁴⁴⁸. Podľa rozhodnutia SDEÚ vo veci *Bodil Lindqvist*⁴⁴⁹ sa však táto výnimka musí vykladať v užšom zmysle, najmä pokiaľ ide o zverejňovanie údajov. Konkrétne sa výnimka pre domáce činnosti netýka sprístupnenia osobných údajov neobmedzenému počtu príjemcov na internete alebo spracúvania údajov, ktoré má profesijné alebo komerčné aspekty (podrobnejšie informácie o tejto veci nájdete v oddieloch 2.1.2, 2.2.2 a 2.3.1).

„Dôvernosť komunikácie“ je ďalším aspektom dôvernosti, na ktorý sa vzťahuje *lex specialis*. Podľa osobitných pravidiel na zabezpečenie dôvernosti elektronických komunikácií podľa smernice o súkromí a elektronických komunikáciách sa vyžaduje, aby členské štáty zakázali počúvanie, odpočúvanie, uchovávanie a iné druhy narušovania alebo sledovania komunikácie a príslušných metadát inými osobami, než sú používatelia, bez súhlasu príslušných používateľov⁴⁵⁰. Vo vnútroštátnom práve sa môžu povoliť výnimky z tejto zásady len z dôvodov národnej bezpečnosti, obrany, prevencie alebo odhalovania trestných činov a len vtedy, ak sú takéto opatrenia nevyhnutné a primerané vzhľadom na sledované ciele⁴⁵¹. Rovnaké pravidlá sa budú uplatňovať aj v rámci budúceho nariadenia o súkromí a elektronických komunikáciách, ale rozsah pôsobnosti tohto právneho aktu sa rozšíri z verejne dostupných elektronických komunikačných služieb aj na komunikáciu vykonávanú prostredníctvom služieb over-the-top (napr. mobilné aplikácie).

Z právnych predpisov RE vyplýva povinnosť zachovávať dôvernosť z pojmu bezpečnosti údajov v článku 7 ods. 1 modernizovaného Dohovoru č. 108, ktorý je venovaný bezpečnosti údajov.

Z hľadiska sprostredkovateľov dôvernosť znamená, že údaje nesmú bez povolenia poskytnúť tretím stranám alebo iným príjemcom. Z hľadiska zamestnancov

447 Všeobecné nariadenie o ochrane údajov, článok 2 ods. 2 písm. c).

448 Tamže.

449 SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003.

450 Smernica o súkromí a elektronických komunikáciách, článok 5 ods. 1.

451 Tamže, článok 15 ods. 1.

prevádzkovateľa alebo sprostredkovateľa si dôvernosť vyžaduje, aby osobné údaje používali len podľa pokynov príslušných nadriadených.

Povinnosť zachovávať dôvernosť musí byť zahrnutá do zmluvy medzi prevádzkovateľmi a ich sprostredkovateľmi. Prevádzkovatelia a sprostredkovatelia budú musieť takisto prijať osobitné opatrenia, ktorými uložia svojim zamestnancom právnu povinnosť zachovávať dôvernosť, ktorá sa bežne zaručuje zahrnutím doložiek o dôvernosti do pracovnej zmluvy zamestnanca.

Porušenie pracovnej povinnosti zachovávania dôvernosti je postihnutelné v rámci trestného práva v mnohých členských štátoch EÚ a zmluvných stranách Dohovoru č. 108.

4.2.3. Oznámenia o porušení ochrany osobných údajov

Porušenie ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu spracúvaných osobných údajov alebo neoprávnenému prístupu k nim⁴⁵². Zatiaľ čo nové technológie, ako je šifrovanie, teraz poskytujú viac možností na zaistenie bezpečnosti spracúvania, porušenia ochrany údajov sú stále bežným javom. Príčinami porušenia ochrany údajov môžu byť náhodné chyby osôb pracujúcich v rámci organizácie až po vonkajšie hrozby, ako sú hackeri a organizácie páchajúce počítačovou trestnú činnosť.

Porušenia ochrany údajov môžu značne poškodzovať práva na súkromie a ochranu údajov jednotlivcov, ktorí v dôsledku porušenia stratia kontrolu nad svojimi osobnými údajmi. Porušenia môžu viesť ku krádeži totožnosti alebo podvodu, finančnej strate alebo materiálnej škode, strate dôvernosti osobných údajov chránených služobným tajomstvom a poškodeniu povesti dotknutej osoby. Pracovná skupina zriadená podľa článku 29 vo svojich usmerneniach o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679 vysvetľuje, že porušenia môžu mať tri typy vplyvu na osobné údaje: zničenie, strata a/alebo zmena⁴⁵³. Okrem povinnosti prijať

452 Všeobecné nariadenie o ochrane údajov, článok 4 bod 12; pozri tiež pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679*, WP250, 30. októbra 2017, s. 8.

453 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679*, WP250, 30. októbra 2017, s. 6.

opatrenia na zaistenie bezpečnosti spracúvania, ako sa vysvetľuje v [oddiele 4.2](#), je rovnako dôležité zabezpečiť, aby prevádzkovatelia prípadné porušenie včas a primeraným spôsobom riešili.

Dozorné orgány a jednotlivci si často neuvedomujú, že došlo k porušeniu ochrany údajov, čo jednotlivcom bráni v prijímaní opatrení na ochranu pred negatívnymi následkami tohto porušenia. **EÚ a RE** za určitých okolností ukládajú prevádzkovateľom oznamovaciu povinnosť s cieľom potvrdiť práva jednotlivcov a obmedziť vplyv porušení ochrany údajov.

Podľa modernizovaného Dohovoru č. 108 **Rady Európy** musia zmluvné strany minimálne vyžadovať, aby prevádzkovatelia oznamovali príslušnému dozornému orgánu porušenia ochrany údajov, ktoré môžu vážne narušiť práva dotknutých osôb. Takéto oznámenie by sa malo vykonať „bezodkladne“⁴⁵⁴.

V **právnych predpisoch EÚ** sa stanovuje podrobný režim upravujúci načasovanie a obsah týchto oznámení⁴⁵⁵. Prevádzkovatelia musia oznámiť určité porušenia údajov dozorným orgánom bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedeli. Ak nedodržia lehotu 72 hodín, oznámenie musí obsahovať vysvetlenie omeškania. Prevádzkovatelia sú oslobodení od oznamovacej povinnosti len vtedy, ak sú schopní preukázať, že nie je pravdepodobné, že porušenie údajov povedie k riziku pre práva a slobody dotknutých fyzických osôb.

V nariadení sa stanovujú minimálne informácie, ktoré sa majú zahrnúť do oznámenia, aby dozorný orgán mohol prijať potrebné opatrenia⁴⁵⁶. Oznámenie musí obsahovať aspoň opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, opis pravdepodobných následkov porušenia a opatrení prijatých prevádzkovateľom na riešenie a zmiernenie jeho dôsledkov. Okrem toho by sa mali poskytnúť meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, aby mohol príslušný dozorný orgán v prípade potreby získať ďalšie informácie.

454 Modernizovaný Dohovor č. 108, článok 7 ods. 2; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 64 – 66.

455 Všeobecné nariadenie o ochrane údajov, článok 33 a 34.

456 Tamže, článok 33 ods. 3.

Ak je pravdepodobné, že porušenie ochrany údajov povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovatelia bez zbytočného odkladu oznámia porušenie ochrany osobných údajov týmto osobám (dotknuté osoby)⁴⁵⁷. Informácie poskytované dotknutým osobám vrátane opisu porušenia ochrany údajov musia byť jasne a jednoducho formulované a musia zahŕňať informácie podobné informáciám, ktoré sa vyžadujú pri oznámeniach dozorným orgánom. Za určitých okolností môžu byť prevádzkovatelia oslobodení od povinnosti oznamovať takéto porušenia dotknutým osobám. Výnimky sa uplatňujú, ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie. Opatrenia, ktoré prevádzkovateľ prijme po porušení s cieľom zabezpečiť, že nedôjde k poškodeniu práv dotknutých osôb, môžu takisto viesť k oslobodeniu prevádzkovateľa od povinnosti informovať dotknuté osoby. Napokon, ak by si oznámenie vyžadovalo neprimerané úsilie zo strany prevádzkovateľa, dotknuté osoby môžu byť informované o porušení inými prostriedkami, napríklad informovaním verejnosti alebo podobným opatrením⁴⁵⁸.

Povinnosť oznamovať porušenia ochrany údajov dozorným orgánom a dotknutým osobám sa vzťahuje na prevádzkovateľov. K porušeniu ochrany údajov však môže dôjsť bez ohľadu na to, či spracúvanie vykonáva prevádzkovateľ alebo sprostredkovateľ. Z tohto dôvodu je nevyhnutné zabezpečiť, aby aj sprostredkovatelia boli povinní oznamovať porušenia ochrany údajov. V takom prípade musia sprostredkovatelia bez zbytočného odkladu oznámiť porušenia ochrany údajov prevádzkovateľovi⁴⁵⁹. Prevádzkovateľ je potom zodpovedný za oznámenie príslušným dozorným orgánom a dotknutým osobám, a to v súlade s uvedenými pravidlami a lehotami.

457 Tamže, článok 34.

458 Tamže, článok 34 ods. 3 písm. c).

459 Tamže, článok 33 ods. 2.

4.3. Pravidlá týkajúce sa zodpovednosti a podpory súladu

Hlavné body

- V záujme zabezpečenia zodpovednosti pri spracúvaní osobných údajov musia prevádzkovatelia a sprostredkovatelia uchovávať záznamy o spracovateľských činnostiach, za ktorých vykonávanie sú zodpovední, a v prípade potreby ich musia poskytnúť dozorným orgánom.
- Vo všeobecnom nariadení o ochrane údajov sa stanovuje niekoľko nástrojov na podporu súladu:
 - určenie zodpovedných osôb v určitých situáciách,
 - vykonanie posúdenia vplyvu pred začatím spracovateľských činností, pri ktorých je pravdepodobné, že budú predstavovať vysoké riziko pre práva a slobody fyzických osôb,
 - predchádzajúcej konzultácie s príslušným dozorným orgánom, ak z posúdenia vplyvu vyplýva, že spracúvanie predstavuje riziká, ktoré nemožno zmierniť,
 - kódexy správania pre prevádzkovateľov a sprostredkovateľov, v ktorých sa špecifikuje uplatňovanie nariadenia v rôznych odvetviach spracúvania,
 - certifikačné mechanizmy, pečate a značky.
- V právnych predpisoch RE sa navrhujú podobné nástroje na podporu súladu s modernizovaným Dohovorom č. 108.

Zásada zodpovednosti je pri zabezpečovaní presadzovania pravidiel ochrany údajov v Európe mimoriadne dôležitá. Prevádzkovateľ je zodpovedný za dodržiavanie súladu s pravidlami ochrany údajov a musí byť schopný tento súlad preukázať. Zodpovednosť by sa mala vyvodiť nielen po tom, ako došlo k porušeniu. Prevádzkovatelia majú proaktívnu povinnosť dodržiavať primerané politiky riadenia údajov vo všetkých fázach spracúvania údajov. V európskych právnych predpisoch o ochrane údajov sa od prevádzkovateľov vyžaduje, aby prijali technické a organizačné opatrenia s cieľom zabezpečiť a preukázať, že spracúvanie sa vykonáva v súlade s právnymi predpismi. Medzi tieto opatrenia patrí určenie zodpovedných osôb, vedenie záznamov a dokumentácie týkajúcej sa spracúvania a vykonávanie posúdení vplyvu na súkromie.

4.3.1. Zodpovedné osoby

Zodpovedné osoby sú osoby, ktoré poskytujú poradenstvo o dodržiavaní pravidiel ochrany údajov v organizáciách, ktoré vykonávajú spracúvanie údajov. Predstavujú „základný kameň zodpovednosti“, keďže uľahčujú dodržiavanie predpisov, pričom konajú aj ako sprostredkovatelia medzi dozornými orgánmi, dotknutými osobami a organizáciou, ktorá ich vymenovala.

Podľa **právnych predpisov RE** sa v článku 10 ods. 1 modernizovaného Dohovoru č. 108 stanovuje všeobecná zodpovednosť prevádzkovateľov a sprostredkovateľov. Od prevádzkovateľov a sprostredkovateľov sa vyžaduje, aby prijali všetky primerané opatrenia na dodržiavanie pravidiel ochrany údajov stanovených v Dohovore a aby boli schopní preukázať, že spracúvanie údajov pod ich kontrolou je v súlade s ustanoveniami Dohovoru. Hoci sa v Dohovore neuvádzajú konkrétne opatrenia, ktoré by mali prevádzkovatelia a sprostredkovatelia prijať, v dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza, že určenie zodpovednej osoby by bolo jedným z možných opatrení, ktoré by pomohli preukázať súlad. Zodpovedným osobám by sa mali poskytnúť všetky prostriedky potrebné na plnenie ich mandátov⁴⁶⁰.

Na rozdiel od právnych predpisov RE, určenie zodpovednej osoby nie je **podľa právnych predpisov EÚ** vždy na voľnom uvážení prevádzkovateľov a sprostredkovateľov, ale za určitých podmienok je povinné. V GDPR sa uznáva, že zodpovedná osoba zohráva v novom systéme riadenia kľúčovú úlohu, a toto nariadenie obsahuje podrobné ustanovenia týkajúce sa určenia, postavenia, povinností a úloh zodpovednej osoby⁴⁶¹.

V GDPR je určenie zodpovednej osoby povinné v troch špecifických prípadoch: ak spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt; ak hlavné činnosti prevádzkovateľa alebo sprostredkovateľa pozostávajú zo spracovateľských operácií, ktoré si vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu, alebo ak hlavné činnosti pozostávajú zo spracúvania osobitných kategórií údajov alebo osobných údajov týkajúcich sa odsúdení za trestné činy a trestných činov vo veľkom rozsahu⁴⁶². Hoci pojmy ako „systematické monitorovanie vo veľkom rozsahu“ a „hlavné činnosti“ nie sú v nariadení vymedzené,

460 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 87.

461 Všeobecné nariadenie o ochrane údajov, články 37 – 39.

462 Tamže, článok 37 ods. 1.

pracovná skupina zriadená podľa článku 29 vydala usmernenia o tom, ako by sa mali vykladať⁴⁶³.

Príklad: Spoločnosti pôsobiace v oblasti sociálnych médií a vyhľadávače sa pravdepodobne budú považovať za prevádzkovateľov, ktorých spracovateľské operácie si vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu. Obchodný model týchto spoločností je založený na spracúvaní veľkého množstva osobných údajov a vytvárajú značné príjmy tým, že ponúkajú cieľené reklamné služby a umožňujú spoločnostiam umiestňovať na stránkach reklamu. Cieľená reklama je spôsob umiestňovania reklamy na základe demografických aspektov a predchádzajúcich nákupov alebo správania spotrebiteľov. Vyžaduje si preto systematické monitorovanie online návykov a správania dotknutých osôb.

Príklad: Nemocnica a zdravotná poisťovňa sú typickými príkladmi prevádzkovateľov, ktorých činnosti pozostávajú z rozsiahleho spracúvania osobitných kategórií osobných údajov. Údaje, ktoré odhaľujú informácie týkajúce sa zdravia osoby, predstavujú osobitné kategórie osobných údajov v rámci právnych predpisov RE a EÚ, a teda si vyžadujú zvýšenú ochranu. V právnych predpisoch EÚ sa ďalej uznávajú ako osobitné kategórie genetické a biometrické údaje. Pokiaľ zdravotnícke zariadenia a poisťovne spracúvajú takéto údaje vo veľkom rozsahu, podľa GDPR sú povinné určiť zodpovednú osobu.

Okrem toho sa v článku 37 ods. 4 GDPR stanovuje, že v prípadoch iných, ako sú tri povinné prípady podľa článku 37 ods. 1, zodpovednú osobu môže určiť, alebo ak sa to vyžaduje v práve Únie alebo práve členského štátu, určí prevádzkovateľ, sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov.

Všetky ostatné organizácie nie sú zo zákona povinné určiť zodpovednú osobu. V GDPR sa však stanovuje, že prevádzkovatelia a sprostredkovatelia sa môžu rozhodnúť, že dobrovoľne určia zodpovednú osobu, pričom sa zároveň členským štátom umožňuje stanoviť povinnosť určenia zodpovednej osoby pre viaceré typy organizácií, než tie, ktoré sú uvedené v nariadení⁴⁶⁴.

463 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia týkajúce sa zodpovedných osôb*, WP 243 rev.01, naposledy revidované a prijaté 5. apríla 2017.

464 Všeobecné nariadenie o ochrane údajov, článok 37 ods. 3 a 4.

Ak prevádzkovateľ určí zodpovednú osobu, musí zabezpečiť, aby bola „riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov“ v rámci organizácie⁴⁶⁵. Zodpovedné osoby by napríklad mali byť zapojené do poskytovania poradenstva týkajúceho sa vykonávania posúdení vplyvu na ochranu údajov a do vytvárania a uchovávanía záznamov o spracovateľských činnostiach v organizácii. Aby zodpovedné osoby mohli účinne vykonávať svoje úlohy, prevádzkovatelia a sprostredkovatelia im musia poskytnúť potrebné zdroje vrátane finančných zdrojov, infraštruktúry a vybavenia. Dodatočné požiadavky zahŕňajú poskytnutie dostatočného času zodpovedným osobám na plnenie ich úloh a priebežnej odbornej prípravy, aby mohli rozvíjať svoje odborné znalosti a udržiavať krok s aktuálnym vývojom v oblasti právnych predpisov o ochrane údajov⁴⁶⁶.

V GDPR sa stanovujú niektoré základné záruky na zabezpečenie nezávislého konania zodpovedných osôb. Prevádzkovatelia a sprostredkovatelia musia zabezpečiť, aby zodpovedné osoby pri výkone svojich úloh súvisiacich s ochranou údajov nedostávali pokyny od spoločnosti vrátane osôb na najvyššej úrovni vedenia. Okrem toho nesmú byť zodpovedné osoby odvolané alebo postihnuté za plnenie svojich úloh⁴⁶⁷. Napríklad, keď zodpovedná osoba odporúča prevádzkovateľovi alebo sprostredkovateľovi, aby vykonal posúdenie vplyvu na ochranu údajov, pretože sa domnieva, že spracúvanie pravdepodobne povedie k vysokému riziku pre dotknuté osoby. Spoločnosť nesúhlasí s odporúčaním zodpovednej osoby, nepovažuje ho za opodstatnené, a preto sa rozhodne nevykonať posúdenie vplyvu. Spoločnosť môže ignorovať odporúčanie, ale nemôže odvolať ani postihnúť zodpovednú osobu za poskytnutie tohto odporúčania.

Úlohy a povinnosti zodpovednej osoby sú uvedené v článku 39 GDPR. Patria k nim požiadavky na poskytovanie informácií a poradenstva spoločnostiam a zamestnancom, ktorí vykonávajú spracúvanie pri plnení svojich povinností podľa právnych predpisov, a na monitorovanie dodržiavania pravidiel EÚ a vnútroštátnych pravidiel ochrany údajov prostredníctvom vykonávania auditov a odbornej prípravy zamestnancov zapojených do spracovateľských operácií. Zodpovedné osoby musia spolupracovať aj s dozorným orgánom a plniť úlohy kontaktného miesta pre dozorné orgány v záležitostiach týkajúcich sa spracúvania údajov, ako je porušenie ochrany údajov.

465 Tamže, článok 38 ods. 1.

466 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia týkajúce sa zodpovedných osôb*, WP 243 rev.01, naposledy revidované a prijaté 5. apríla 2017, bod 3.1.

467 Všeobecné nariadenie o ochrane údajov, článok 38 ods. 2 a 3.

Pokiaľ ide o osobné údaje, ktoré spracúvajú inštitúcie a orgány EÚ, v nariadení č. 45/2001 sa stanovuje, že každá inštitúcia a orgán Únie musí určiť zodpovednú osobu. Zodpovedná osoba je poverená zabezpečením toho, aby sa ustanovenia nariadenia správne uplatňovali v rámci inštitúcií a orgánov EÚ a aby dotknuté osoby a prevádzkovatelia boli informovaní o svojich právach a povinnostiach⁴⁶⁸. Zodpovedá aj za odpovedanie na žiadosti EDPS a v prípade potreby s ním spolupracuje. Podobne ako GDPR, aj nariadenie č. 45/2001 obsahuje ustanovenia o nezávislosti zodpovedných osôb pri plnení ich úloh a o potrebe poskytnúť im potrebný personál a zdroje⁴⁶⁹. Zodpovedné osoby musia byť informované pred tým, ako inštitúcia alebo orgán EÚ (alebo oddelenia týchto organizácií) vykonajú akékoľvek spracovateľské operácie, a musia viesť register všetkých oznámených spracovateľských operácií⁴⁷⁰.

4.3.2. Záznamy o spracovateľských činnostiach

Na to, aby spoločnosti boli schopné preukázať súlad a niešť zodpovednosť, sú často zo zákona povinné zdokumentovať svoje činnosti a zaznamenať ich. Dôležitým príkladom je daňové právo a audit, pri ktorých sa vyžaduje, aby všetky spoločnosti viedli rozsiahlu dokumentáciu a záznamy. Stanovenie podobných požiadaviek je dôležité aj v iných právnych oblastiach, najmä v právnych predpisoch o ochrane údajov, keďže vedenie záznamov je dôležitým prostriedkom na uľahčenie dodržiavania pravidiel ochrany údajov. V **právnych predpisoch** EÚ sa preto stanovuje, že prevádzkovatelia alebo ich zástupcovia musia viesť záznamy o spracovateľských činnostiach, za ktorých vykonávanie sú zodpovední⁴⁷¹. Cieľom tejto povinnosti je zabezpečiť, aby dozorné orgány mali v prípade potreby k dispozícii potrebnú dokumentáciu, ktorá im umožní potvrdiť zákonnosť spracúvania.

Informácie, ktoré sa majú zdokumentovať, zahŕňajú:

- meno/názov a kontaktné údaje prevádzkovateľa a prípadne spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby,
- účely spracúvania,

468 Pozri článok 24 ods. 1 nariadenia (ES) č. 45/2001 pre úplný zoznam úloh zodpovednej osoby.

469 Nariadenie (ES) č. 45/2001, článok 24 ods. 6 a 7.

470 Tamže, články 25 a 26.

471 Všeobecné nariadenie o ochrane údajov, článok 30.

- opis kategórií dotknutých osôb a kategórií osobných údajov týkajúcich sa spracúvania,
- informácie o kategóriách príjemcov, ktorým sa osobné údaje poskytnú,
- informácie o tom, či sa vykonali alebo sa vykonajú prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám,
- podľa možnosti predpokladané lehoty na vymazanie rôznych kategórií údajov, ako aj prehľad technických opatrení prijatých na zaistenie bezpečnosti spracúvania⁴⁷².

Povinnosť viesť záznamy o spracovateľských činnostiach podľa GDPR sa týka nielen prevádzkovateľov, ale aj sprostredkovateľov. Ide o dôležitý vývoj, keďže pred prijatím tohto nariadenia sa zmluva uzavretá medzi prevádzkovateľom a sprostredkovateľom primárne vzťahovala na povinnosti sprostredkovateľa. Ich povinnosť vedenia záznamov je teraz priamo stanovená v právnych predpisoch.

V GDPR sa stanovuje výnimka z tejto povinnosti. Požiadavka viesť záznamy sa nevzťahuje na podnik alebo organizáciu (prevádzkovateľa alebo sprostredkovateľa), ktorá zamestnáva menej ako 250 osôb. Výnimka však platí za predpokladu, že dotknutá organizácia nevykonáva spracúvanie, ktoré by mohlo viesť k riziku pre práva a slobody dotknutých osôb, že spracúvanie je len príležitostné a že nezasahuje osobitné kategórie údajov podľa článku 9 ods. 1 ani osobné údaje týkajúce sa odsúdení za trestné činy a trestných činov podľa článku 10.

Vedenie záznamov o spracovateľských činnostiach by malo umožniť prevádzkovateľom a sprostredkovateľom preukázať súlad s nariadením. Malo by tiež umožniť dozorným orgánom monitorovať zákonnosť spracúvania. Ak dozorný orgán požiada o prístup k týmto záznamom, prevádzkovatelia a sprostredkovatelia sú povinní spolupracovať a sprístupniť ich.

472 Tamže, článok 30 ods. 1.

4.3.3. Posúdenie vplyvu na ochranu údajov a predchádzajúca konzultácia

Spracovateľské operácie predstavujú určité inherentné riziká pre práva jednotlivcov. Osobné údaje sa môžu stratiť, sprístupniť neoprávneným stranám alebo spracúvať nezákonným spôsobom. Riziká sa, samozrejme, líšia v závislosti od povahy a rozsahu spracúvania. Operácie vo veľkom rozsahu, ktoré zahŕňajú spracúvanie citlivých údajov, majú napríklad oveľa vyšší stupeň rizika pre dotknuté osoby v porovnaní s možnými rizikami, keď malá spoločnosť spracúva adresy a osobné telefónne čísla svojich zamestnancov.

Keďže sa vyvíjajú nové technológie a spracúvanie sa stáva čoraz zložitejším, prevádzkovatelia musia takéto riziká riešiť preskúmaním pravdepodobného vplyvu plánovaného spracúvania pred jeho začatím. Organizáciám to umožňuje vopred správne identifikovať, riešiť a zmierňovať riziká a výrazne obmedziť pravdepodobnosť negatívneho vplyvu na jednotlivcov v dôsledku spracúvania.

Posúdenie vplyvu na ochranu údajov sa rieši v **právnych predpisoch RE, ako aj EÚ**. V právnom rámci RE sa v článku 10 ods. 2 modernizovaného Dohovoru č. 108 vyžaduje, aby zmluvné strany zabezpečili, aby prevádzkovatelia a sprostredkovatelia „preskúmali pravdepodobný vplyv zamýšľaného spracúvania údajov na práva a základné slobody dotknutých osôb pred začatím takeéhoto spracúvania“ a po posúdení navrhli spracúvanie tak, aby sa predišlo rizikám spojeným so spracúvaním alebo aby sa tieto riziká minimalizovali.

V právnych predpisoch EÚ sa ukladá podobná, podrobnejšia povinnosť prevádzkovateľom, ktorí patria do rozsahu pôsobnosti GDPR. V článku 35 sa stanovuje, že posúdenie vplyvu sa musí vykonať, ak je pravdepodobné, že spracúvanie povedie k vysokému riziku pre práva a slobody fyzických osôb. V nariadení sa nevymedzuje, ako sa má posudzovať pravdepodobnosť rizika, ale skôr sa uvádza, o aké riziká by mohlo ísť⁴⁷³. Obsahuje zoznam spracovateľských operácií, ktoré sa považujú za vysoko rizikové a pri ktorých je mimoriadne potrebné predchádzajúce posúdenie vplyvu, a to v prípadoch, keď:

- osobné údaje sa spracúvajú na účely prijímania rozhodnutí týkajúcich sa fyzických osôb, a to na základe akéhokoľvek systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb (profilovanie),

473 Všeobecné nariadenie o ochrane údajov, preambula, odôvodnenie 75.

- citlivé údaje alebo osobné údaje týkajúce sa odsúdení za trestné činy a trestných činov sa spracúvajú vo veľkom rozsahu,
- spracúvanie zahŕňa rozsiahle systematické monitorovanie verejne prístupných miest.

Dozorné orgány musia prijať a uverejniť zoznam spracovateľských operácií, ktoré podliehajú požiadavke posúdenia vplyvu. Môžu tiež vypracovať zoznam spracovateľských operácií oslobodených od tejto povinnosti⁴⁷⁴.

Ak sa vyžaduje posúdenie vplyvu, prevádzkovatelia musia posúdiť nevyhnutnosť a primeranosť spracúvania a možné riziká pre práva jednotlivcov. Posúdenie vplyvu musí obsahovať aj plánované bezpečnostné opatrenia na riešenie zistených rizík. Pri zostavovaní týchto zoznamov sú dozorné orgány členských štátov povinné spolupracovať navzájom a s Európskym výborom pre ochranu údajov. Zabezpečí sa tým konzistentný prístup v rámci celej EÚ k tým operáciám, ktoré si vyžadujú posúdenie vplyvu, a prevádzkovatelia budú podliehať podobným požiadavkám bez ohľadu na to, kde sa nachádzajú.

Ak sa po posúdení vplyvu ukáže, že spracúvanie povedie k vysokému riziku pre práva jednotlivcov a nie sú prijaté žiadne opatrenia na zmiernenie rizika, prevádzkovateľ sa pred začatím spracovateľskej operácie poradí s príslušným dozorným orgánom⁴⁷⁵.

Pracovná skupina zriadená podľa článku 29 vydala usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a o tom, ako určiť, či spracúvanie pravdepodobne povedie k vysokému riziku⁴⁷⁶. Vypracovala deväť kritérií, ktoré majú pomôcť určiť, či sa v konkrétnom prípade vyžaduje posúdenie vplyvu na ochranu údajov⁴⁷⁷:

1. hodnotenie alebo pridelenie bodov;
2. automatizované rozhodovanie s právnym alebo podobne závažným účinkom;
3. systematické monitorovanie;
4. citlivé údaje;
5. údaje spracúvané vo veľkom rozsahu;
6. spájané alebo kombinované

474 Tamže, článok 35 ods. 4 a 5.

475 Tamže, článok 36 ods. 1; Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“*, WP 248 rev.01, Brusel, 4. októbra 2017.

476 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“*, WP 248 rev.01, Brusel, 4. októbra 2017.

477 Tamže, s. 9 – 11.

súbory údajov; 7. údaje týkajúce sa zraniteľných dotknutých osôb; 8. inovačné využitie alebo uplatňovanie nových technologických alebo organizačných riešení; 9. keď samotné spracúvanie „bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu“. Pracovná skupina zriadená podľa článku 29 zaviedla všeobecné pravidlo, že spracovateľské operácie, ktoré spĺňajú menej ako dve kritériá, predstavujú nižšie úrovne rizika a nevyžadujú si posúdenie ochrany údajov, zatiaľ čo tie, ktoré spĺňajú dve alebo viaceré kritériá, si takéto posúdenie vyžadujú. V prípadoch, keď nie je jasné, či sa vyžaduje posúdenie vplyvu na ochranu údajov, pracovná skupina zriadená podľa článku 29 odporúča vykonať takéto posúdenie, pretože je to „užitočný nástroj, ako pomôcť prevádzkovateľom dodržiavať právne predpisy o ochrane údajov“⁴⁷⁸. Ak sa zavedie nová technológia spracúvania údajov, je dôležité, aby sa vykonalo posúdenie vplyvu na ochranu údajov⁴⁷⁹.

4.3.4. Kódexy správania

Kódexy správania sa majú používať vo viacerých odvetviach s cieľom opísať a spresniť uplatňovanie GDPR v konkrétnych odvetviach. Vytvorenie takýchto kódexov umožňuje prevádzkovateľom a sprostredkovateľom osobných údajov výrazne zlepšiť dodržiavanie súladu a zlepšiť vykonávanie pravidiel EÚ na ochranu údajov. Odborné znalosti členov odvetvia pomôžu nachádzať riešenia, ktoré sú praktické, a preto sa pravdepodobne uplatnia. V GDPR sa uznáva význam takýchto kódexov pri účinnom uplatňovaní právnych predpisov o ochrane údajov, a preto sa vyzývajú členské štáty, dozorné orgány, Komisia a Európsky výbor pre ochranu údajov, aby podporili vypracovanie kódexov správania, ktoré majú prispieť k správaniu uplatňovaniu nariadenia v celej EÚ⁴⁸⁰. V týchto kódexoch by sa mohlo spresniť uplatňovanie tohto nariadenia v konkrétnych odvetviach vrátane riešenia otázok, ako je získavanie osobných údajov, informovanie dotknutých osôb a verejnosti, ako aj uplatňovanie práv dotknutých osôb.

Na zabezpečenie toho, aby kódexy správania boli v súlade s pravidlami stanovenými podľa GDPR, sa tieto kódexy musia pred prijatím predložiť príslušnému dozornému orgánu. Dozorný orgán potom vydá stanovisko k tomu, či predložený návrh kódexu podporuje súlad s nariadením, a ak dospeje k záveru, že kódex poskytuje primerané záruky, kódex schváli⁴⁸¹. Dozorné orgány musia uverejniť schválené kódexy správa-

⁴⁷⁸ Tamže, s. 9.

⁴⁷⁹ Tamže.

⁴⁸⁰ Všeobecné nariadenie o ochrane údajov, článok 40 ods. 1.

⁴⁸¹ Tamže, článok 40 ods. 5.

nia, ako aj kritériá, na základe ktorých ich schválili. Ak sa návrh kódexu správania týka spracovateľských činností vo viacerých členských štátoch, príslušný dozorný orgán pred schválením návrhu kódexu, zmeny alebo rozšírenia predloží kódex Európskemu výboru pre ochranu údajov, ktorý poskytne stanovisko o súlade kódexu s GDPR. Komisia môže prostredníctvom vykonávacích aktov rozhodnúť, že schválený kódex správania, ktorý jej bol predložený, má všeobecnú platnosť v rámci Únie.

Dodržiavanie kódexu správania poskytuje významné výhody pre dotknuté osoby, ako aj pre prevádzkovateľov aj sprostredkovateľov. Takéto kódexy poskytujú podrobné usmernenia, ktorými sa právne požiadavky prispôbujú konkrétnym odvetviam a podporuje sa transparentnosť spracovateľských činností. Prevádzkovatelia a sprostredkovatelia môžu používať kódexy aj ako preukázateľný dôkaz ich dodržiavania právnych predpisov EÚ a ako prostriedok na zlepšenie ich dobrého mena na verejnosti ako organizácie, ktoré pri svojich operáciách uprednostňujú ochranu údajov a zaväzujú sa k nej. Schválené kódexy správania spolu so záväznými a vykonateľnými záväzkami je možné použiť ako primerané záruky pri prenose údajov do tretích krajín. Na zabezpečenie toho, aby organizácie riadiace sa kódexom správania tento kódex aj skutočne dodržiavali, sa môže určiť osobitný orgán (akreditovaný príslušným dozorným orgánom), aby monitoroval a zabezpečoval dodržiavanie kódexu. Aby tento orgán mohol účinne plniť svoje úlohy, musí byť nezávislý, mať preukázateľné odborné znalosti v oblastiach, na ktoré sa vzťahuje kódex správania, a mať transparentné postupy a štruktúry, ktoré mu umožnia vybavovať sťažnosti týkajúce sa porušení kódexu⁴⁸².

V rámci právnych predpisov RE sa v modernizovanom Dohovore č. 108 stanovuje, že úroveň ochrany údajov zaručená vnútroštátnymi právnymi predpismi sa môže užitočne posilniť dobrovoľnými regulačnými opatreniami, ako sú kódexy osvedčených postupov alebo kódexy výkonu povolania. Tieto opatrenia však podľa modernizovaného Dohovoru č. 108 predstavujú len dobrovoľné opatrenia: na zavedenie takýchto opatrení sa nevzťahuje žiadna právna povinnosť, aj keď ich zavedenie je vhodné, a samotné takéto opatrenia nepostačujú na zabezpečenie úplného súladu s Dohovorom⁴⁸³.

482 Tamže, článok 41 ods. 1 a 2.

483 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 33.

4.3.5. Certifikácia

Okrem kódexov správania sú ďalším spôsobom, ako môžu prevádzkovatelia a sprostredkovatelia preukázať súlad s GDPR, certifikačné mechanizmy a pečate a značky ochrany údajov. V nariadení sa na tento účel stanovuje dobrovoľný systém certifikácie, v rámci ktorého môžu určité subjekty alebo dozorné orgány vydávať certifikácie. Prevádzkovatelia a sprostredkovatelia, ktorí sa rozhodnú dodržiavať certifikačný mechanizmus, sa môžu zviditeľniť a získať dôveryhodnosť, pretože certifikácie, pečate a značky umožňujú dotknutým osobám rýchlo posúdiť úroveň ochrany údajov v danej organizácii. Je dôležité uviesť, že skutočnosť, že prevádzkovateľ alebo sprostredkovateľ získal takúto certifikáciu, neznižuje rozsah jeho povinnosti a zodpovednosti pri plnení všetkých požiadaviek vyplývajúcich z nariadenia.

4.4. Špecificky navrhnutá a štandardná ochrana údajov

Špecificky navrhnutá ochrana údajov

Podľa **právnych predpisov EÚ** sa vyžaduje, aby prevádzkovatelia zaviedli opatrenia na účinné vykonávanie zásad ochrany údajov a aby začlenili nevyhnuté záruky s cieľom splniť požiadavky nariadenia a chrániť práva dotknutých osôb⁴⁸⁴. Tieto opatrenia by sa mali zavádzať tak v čase spracúvania, ako aj pri určovaní prostriedkov spracúvania. Pri zavádzaní týchto opatrení musí prevádzkovateľ zohľadniť najnovšie poznatky, náklady na vykonávanie, povahu, rozsah a účely spracúvania osobných údajov a riziká a závažnosť pre práva a slobody dotknutej osoby⁴⁸⁵.

Podľa **právnych predpisov RE** sa vyžaduje, aby prevádzkovatelia a sprostredkovatelia pred začatím spracúvania posúdili pravdepodobný účinok spracúvania osobných údajov na práva a slobody dotknutých osôb. Okrem toho sú prevádzkovatelia a sprostredkovatelia povinní navrhnuť spracúvanie údajov takým spôsobom, aby sa zabránilo riziku zasahovania do týchto práv a slobôd alebo aby sa toto riziko minimalizovalo, a zaviesť technické a organizačné opatrenia, pri ktorých sa zohľadnia

⁴⁸⁴ Všeobecné nariadenie o ochrane údajov, článok 25 ods. 1.

⁴⁸⁵ Pozri dokument pracovnej skupiny zriadenej podľa článku 29 (2017), *Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“*, WP 248 rev.01, Brusel, 4. októbra 2017. Pozri tiež ENISA (2015), *Privacy and Data Protection by Design—from policy to engineering*, 12. januára 2015.

dôsledky práva na ochranu osobných údajov vo všetkých fázach spracúvania údajov⁴⁸⁶.

Štandardná ochrana údajov

Podľa **právnych predpisov EÚ** sa vyžaduje, aby prevádzkovateľ zaviedol primerané opatrenia s cieľom zabezpečiť, aby sa štandardne spracúvali iba osobné údaje, ktoré sú nevyhnutné na príslušné účely. Táto povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť⁴⁸⁷. Takýmto opatrením sa musí napríklad zabezpečiť, že nie všetci zamestnanci prevádzkovateľa majú prístup k osobným údajom dotknutých osôb. EDPS vypracoval ďalšie usmernenia v dokumente *Necessity Toolkit*⁴⁸⁸.

Podľa **právnych predpisov RE** sa vyžaduje, aby prevádzkovatelia a sprostredkovatelia zaviedli technické a organizačné opatrenia s cieľom zväziť dôsledky práva na ochranu údajov a zaviedli technické a organizačné opatrenia, v ktorých sa zohľadnia dôsledky práva na ochranu osobných údajov vo všetkých fázach spracúvania údajov⁴⁸⁹.

V roku 2016 agentúra ENISA uverejnila správu o dostupných nástrojoch a službách na ochranu súkromia⁴⁹⁰. Okrem iných úvah sa v tomto posúdení uvádza index kritérií a parametrov, ktoré slúžia ako ukazovatele dobrých alebo zlých postupov v oblasti ochrany súkromia. Zatiaľ čo niektoré kritériá sa priamo týkajú ustanovení GDPR, ako je využívanie pseudonymizácie a schválených certifikačných mechanizmov, iné predstavujú inovatívne iniciatívy na zabezpečenie špecificky navrhutej a štandardnej ochrany súkromia. Napríklad kritérium použiteľnosti, hoci priamo nesúvisí so súkromím, môže zlepšovať ochranu súkromia, keďže umožní rozšírenejšie používanie nástroja alebo služby na ochranu súkromia. Nástroje na ochranu súkromia, ktoré sa v praxi ťažko používajú, môže široká verejnosť v skutočnosti používať len vo veľmi nízkej miere, a to aj napriek tomu, že poskytujú veľmi dobré záruky ochrany súkromia. Okrem toho má kľúčový význam kritérium vyspelosti a stability nástroja

486 Modernizovaný Dohovor č. 108, článok 10 ods. 2 a 3; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 89.

487 Všeobecné nariadenie o ochrane údajov, článok 25 ods. 2.

488 Európsky dozorný úradník pre ochranu údajov (EDPS), (2017), *Necessity Toolkit*, Brusel, 11. apríla 2017.

489 Modernizovaný Dohovor č. 108, článok 10 ods. 2; dôvodová správa k modernizovanému Dohovoru č. 108, ods. 89.

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools*, 20. decembra 2016.

na ochranu súkromia, teda spôsob, akým sa tento nástroj časom vyvíja a reaguje na existujúce alebo nové výzvy týkajúce sa súkromia. Iné technológie na zvyšovanie súkromia, napríklad v súvislosti s bezpečnou komunikáciou, zahŕňajú šifrovanie bez medzifáz (komunikácia, pri ktorej môžu správy čítať len ľudia, ktorí komunikujú); šifrovanie klient-server (šifrovanie komunikačného kanála zriadeného medzi klientom a serverom); autentifikáciu (overenie totožnosti komunikujúcich strán); a anonymnú komunikáciu (žiadna tretia strana nemôže identifikovať komunikujúce strany).

5

Nezávislý dohľad

EÚ	Zahrnuté témy	RE
Charta, článok 8 ods. 3 Zmluva o fungovaní EÚ, článok 16 ods. 2 Všeobecné nariadenie o ochrane údajov, články 51 – 59 SDEÚ, C-518/07, <i>Európska komisia/ Spolková republika Nemecko</i> [VK], 2010 SDEÚ, C-614/10, <i>Európska komisia/ Rakúska republika</i> [VK], 2012 SDEÚ, C-288/12, <i>Európska komisia/ Maďarsko</i> [VK], 2014 SDEÚ, C-362/14, <i>Maximillian Schrems/ Data Protection Commissioner</i> [VK], 2015	Dozorné orgány	Modernizovaný Dohovor č. 108, článok 15
Všeobecné nariadenie o ochrane údajov, články 60 – 67	Spolupráca medzi dozornými orgánmi	Modernizovaný Dohovor č. 108, články 16 – 21
Všeobecné nariadenie o ochrane údajov, články 68 – 76	Európsky výbor pre ochranu údajov	

Hlavné body

- Nezávislý dohľad je základným prvkom európskeho práva v oblasti ochrany údajov a je zakotvený v článku 8 ods. 3 Charty.
- V záujme zabezpečenia účinnej ochrany údajov musia byť na základe vnútroštátnych právnych predpisov zriadené nezávislé dozorné orgány.
- Dozorné orgány musia konať úplne nezávisle, pričom ich nezávislosť musí byť zaručená v ustanovujúcom právnom predpise a zohľadnená v osobitnej organizačnej štruktúre dozorného orgánu.
- Dozorné orgány majú osobitné právomoci a úlohy. Patria k nim okrem iného:
 - monitorovanie a podpora ochrany údajov na vnútroštátnej úrovni,
 - poskytovanie poradenstva dotknutým osobám a prevádzkovateľom, ako aj štátnej správe a všeobecnej verejnosti,
 - prijímanie sťažností a pomoc dotknutým osobám v prípadoch podozrenia z porušenia práv na ochranu údajov,
 - vykonávanie dohľadu nad prevádzkovateľmi a sprostredkovateľmi.
- Dozorné orgány majú tiež právomoc v prípade potreby zasiahnuť formou:
 - výstrahy, pokarhania, a dokonca udelenia pokuty prevádzkovateľom a sprostredkovateľom,
 - vydania príkazu na úpravu, zablokovanie alebo výmaz údajov,
 - vydania zákazu spracúvania alebo uloženia správnej pokuty,
 - postúpenia veci na súd.
- Keďže spracúvanie osobných údajov často zahŕňa prevádzkovateľov, sprostredkovateľov a dotknuté osoby nachádzajúce sa v rôznych štátoch, dozorné orgány sú povinné navzájom spolupracovať v cezhraničných otázkach s cieľom zabezpečiť účinnú ochranu jednotlivcov v Európe.
- V EÚ sa vo všeobecnom nariadení o ochrane údajov stanovuje mechanizmus jedného kontaktného miesta pre prípady cezhraničného spracúvania. Niektoré spoločnosti vykonávajú činnosti cezhraničného spracúvania v dôsledku toho, že spracúvajú osobné údaje v rámci činnosti prevádzkarní vo viac ako jednom členskom štáte alebo v rámci jedinej prevádzkarnie v Únii, pričom však týmto spracúvaním podstatne ovplyvňujú dotknuté osoby vo viac ako jednom členskom štáte. V rámci tohto mechanizmu budú takéto spoločnosti spolupracovať len s jedným národným dozorným orgánom pre ochranu údajov.

- Mechanizmus spolupráce a konzistentnosti umožní koordinovaný prístup medzi všetkými dozornými orgánmi, ktoré sú zapojené do konkrétneho prípadu. Vedúci dozorný orgán – pre hlavnú alebo jedinou prevádzkareň – bude konzultovať svoj návrh rozhodnutia s ostatnými dotknutými dozornými orgánmi a predloží im ho.
- Podobne ako v prípade súčasnej pracovnej skupiny zriadenej podľa článku 29 bude dozorný orgán každého členského štátu a Európsky dozorný úradník pre ochranu údajov (EDPS) súčasťou Európskeho výboru pre ochranu údajov.
- Medzi úlohy Európskeho výboru pre ochranu údajov patrí napríklad monitorovanie správneho uplatňovania nariadenia, poskytovanie poradenstva Komisii v príslušných otázkach a vydávanie stanovísk, usmernení alebo najlepších postupov týkajúcich sa rôznych tém.
- Hlavný rozdiel spočíva v tom, že Európsky výbor pre ochranu údajov nebude vydávať len stanoviská, ako to bolo podľa smernice 95/46/ES. Bude vydávať aj záväzné rozhodnutia v prípadoch, ak dozorný orgán vznesie relevantnú a odôvodnenú námietku v prípadoch jednotných kontaktných miest; ak existujú protichodné názory na to, ktorý dozorný orgán je vedúci; a napokon, ak príslušný dozorný orgán nepožiadá EDPB o stanovisko alebo nepostupuje podľa stanoviska Výboru. Cieľom je zabezpečiť konzistentné uplatňovanie nariadenia vo všetkých členských štátoch.

Nezávislý dohľad je základným prvkom európskeho práva v oblasti ochrany údajov. V právnych predpisoch EÚ, ako aj v právnych predpisoch RE sa existencia nezávislých dozorných orgánov považuje za nevyhnutnú na účinnú ochranu práv a slobôd jednotlivcov pri spracúvaní ich osobných údajov. Keďže k spracúvaniu údajov v súčasnosti dochádza neustále a pre jednotlivcov je čoraz zložitejšie ho pochopiť, tieto orgány sú strážnikmi digitálneho veku. V EÚ sa existencia nezávislých dozorných orgánov považuje za jeden z najdôležitejších prvkov práva na ochranu osobných údajov zakotveného v primárnom práve EÚ. V článku 8 ods. 3 Charty a článku 16 ods. 2 ZFEÚ sa uznáva ochrana osobných údajov ako základné právo a potvrdzuje, že dodržiavanie pravidiel ochrany údajov musí podliehať kontrole nezávislého orgánu.

Význam nezávislého dohľadu nad právnymi predpismi na ochranu údajov je uznávaný aj judikatúrou.

Príklad: V rozsudku vo veci *Schrems*⁴⁹¹ sa SDEÚ zaoberal otázkou, či zaslanie osobných údajov do Spojených štátov (USA) na základe prvej dohody o Safe Harbour medzi EÚ a USA bolo v súlade s právnymi predpismi EÚ o ochrane údajov, vzhľadom na odhalenia pána Edwarda Snowdena týkajúce

491 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

sa hromadného sledovania americkou Národnou bezpečnostnou agentúrou. K prenosu osobných údajov do USA dochádzalo na základe rozhodnutia Európskej komisie prijatého v roku 2000, ktorým sa umožnil prenos osobných údajov z EÚ organizáciám v USA, ktoré osvedčia, že dodržiavajú zásady Safe Harbour, keďže tento systém zabezpečuje primeranú úroveň ochrany osobných údajov. Írsky dozorný orgán zamietol žiadosť o prešetrovanie sťažnosti týkajúcej sa zákonnosti prenosu údajov po Snowdenových odhaleniach z dôvodu, že existencia rozhodnutia Komisie o primeranosti režimu ochrany údajov v USA, ktorý sa odráža v zásadách Safe Harbour („rozhodnutie o Safe Harbour“), mu bráni v ďalšom vyšetrení sťažnosti.

SDEÚ však rozhodol, že existencia rozhodnutia Komisie, ktorým sa umožňujú prenosy údajov do tretích krajín, ktoré zabezpečujú primeranú úroveň ochrany, nevylučuje alebo neobmedzuje právomoci vnútroštátnych dozorných orgánov. SDEÚ konštatoval, že právomoci týchto orgánov monitorovať a zabezpečovať súlad s pravidlami EÚ v oblasti ochrany údajov vyplývajú z primárneho práva EÚ, najmä z článku 8 ods. 3 Charty a článku 16 ods. 2 ZFEÚ. „Zriadenie nezávislých dozorných orgánov v členských štátoch tak predstavuje [...] základný prvok rešpektovania ochrany osôb v súvislosti so spracovaním osobných údajov⁴⁹².“

SDEÚ preto rozhodol, že aj v prípade, keď prenos osobných údajov podlieha rozhodnutiu Komisie o primeranosti, ak sa národnému dozornému orgánu podá sťažnosť, orgán ju musí preskúmať s náležitou starostlivosťou. Dozorný orgán môže sťažnosť zamietnuť, ak zistí, že je neopodstatnená. V takom prípade SDEÚ zdôraznil, že právo na účinný súdny prostriedok nápravy si vyžaduje, aby jednotlivci mali možnosť napadnúť takéto rozhodnutie na vnútroštátnych súdoch, ktoré môžu vec predložiť SDEÚ na prejudiciálne rozhodnutie o platnosti rozhodnutia Komisie. Ak dozorný orgán uzná sťažnosť za dôvodnú, musí mať možnosť začať súdne konanie a predložiť vec vnútroštátnym súdom. Vnútroštátne súdy môžu prípad postúpiť SDEÚ, keďže je jediným orgánom s právomocou rozhodovať o platnosti rozhodnutia Komisie o primeranosti⁴⁹³.

492 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015, bod 41.

493 Tamže, body 53 – 66.

SDEÚ následne preskúmal platnosť rozhodnutia o Safe Harbour s cieľom stanoviť, či bol systém prenosov v súlade s pravidlami EÚ na ochranu údajov. Dospel k záveru, že článkom 3 rozhodnutia o Safe Harbour sa obmedzujú právomoci vnútroštátnych dozorných orgánov (podľa smernice o ochrane údajov) prijímať opatrenia na zabránenie prenosu údajov v prípade neprimeranej úrovne ochrany osobných údajov v USA. Vzhľadom na význam nezávislých dozorných orgánov pri zabezpečovaní dodržiavania právnych predpisov v oblasti ochrany údajov SDEÚ rozhodol, že podľa smernice o ochrane údajov a v spojení s Chartou Komisia nebola oprávnená takýmto spôsobom obmedziť právomoci nezávislých dozorných orgánov. Obmedzenie právomocí dozorných orgánov bolo jedným z dôvodov, prečo SDEÚ vyhlásil rozhodnutie o Safe Harbour za neplatné.

Podľa európskeho práva sa teda vyžaduje nezávislý dohľad ako dôležitý mechanizmus na zabezpečenie účinnej ochrany údajov. Nezávislé dozorné orgány sú prvým kontaktným miestom pre dotknuté osoby v prípadoch porušenia ochrany súkromia⁴⁹⁴. Podľa právnych predpisov EÚ a právnych predpisov RE je zriadenie dozorných orgánov povinné. Oba právne rámce opisujú úlohy a právomoci týchto orgánov podobné úlohám a právomociam uvedeným v GDPR. V zásade by preto dozorné orgány mali fungovať rovnako podľa právnych predpisov EÚ, ako aj právnych predpisov RE⁴⁹⁵.

5.1. Nezávislosť

Podľa **právnych predpisov EÚ** aj **právnych predpisov RE** sa požaduje, aby každý dozorný orgán konal pri plnení svojich úloh a pri výkone svojich právomocí úplne nezávisle⁴⁹⁶. Nezávislosť dozorného orgánu a jeho členov, ako aj zamestnancov od priamych alebo nepriamych vonkajších vplyvov má zásadný význam pri zaručovaní úplnej objektívnosti pri rozhodovaní o otázkach ochrany údajov. Právny predpis, ktorý je základom na vytvorenie dozorného orgánu, musí nielen obsahovať ustanovenia, ktorými sa osobitne zaručí jeho nezávislosť, ale nezávislosť musí byť zrejmä aj z organizačnej štruktúry orgánu. V roku 2010 sa SDEÚ prvýkrát zaoberal otázkou

494 Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. d).

495 Tamže, článok 51; modernizovaný Dohovor č. 108, článok 15.

496 Všeobecné nariadenie o ochrane údajov, článok 52 ods. 1; modernizovaný Dohovor č. 108, článok 15 ods. 5.

rozsahu požiadavky na nezávislosť dozorných orgánov pre ochranu údajov⁴⁹⁷. Zvýraznené príklady ilustrujú, ako SDEÚ vymedzuje pojem „úplná nezávislosť“.

Príklad: Vo veci *Európska Komisia/Spolková republika Nemecko*⁴⁹⁸ Európska komisia požiadala SDEÚ, aby vyhlásil, že Nemecko nesprávne transponovalo požiadavku „úplnej nezávislosti“ dozorných orgánov zodpovedných za zabezpečenie ochrany údajov, čím nesplnilo požiadavky vyplývajúce z článku 28 ods. 1 smernice o ochrane údajov. Podľa názoru Komisie problém spočíval v tom, že Nemecko ustanovilo štátny dohľad nad orgánmi zodpovednými za monitorovanie spracúvania osobných údajov mimo verejného sektora v rôznych spolkových krajinách (*Länder*).

SDEÚ zdôraznil, že výklad výrazu „úplne nezávisle“ musí zohľadniť samotné znenie uvedeného ustanovenia, ako aj ciele a systematicku právnych predpisov EÚ o ochrane údajov⁴⁹⁹. SDEÚ zdôraznil, že dozorné orgány sú „strážcovia“ základných práv týkajúcich sa spracúvania osobných údajov. Ich zriadenie v členských štátoch je preto považované „za nevyhnutný prvok ochrany jednotlivcov v súvislosti so spracovaním osobných údajov“⁵⁰⁰. SDEÚ dospel k záveru, že „pri vykonávaní svojich úloh musia dozorné orgány konať objektívne a nestranné. Na tento účel musia byť oslobodené od akéhokoľvek vonkajšieho vplyvu vrátane priameho či nepriameho vplyvu štátu alebo spolkových krajín, a teda nielen od vplyvu kontrolovaných subjektov“⁵⁰¹.

SDEÚ takisto konštatoval, že význam výrazu „úplná nezávislosť“ by sa mal vykladať so zreteľom na nezávislosť EDPS, ako je vymedzená v nariadení o ochrane údajov inštitúciami EÚ. V tomto nariadení sa pod pojmom nezávislosť uvádza, že EDPS nemôže od nikoho požadovať ani prijímať pokyny.

V súlade s tým SDEÚ skonštatoval, že nemecké dozorné orgány neboli úplne nezávislé v zmysle právnych predpisov EÚ o ochrane údajov, keďže boli podrobené dohľadu zo strany štátnych orgánov.

497 Pozri FRA (2010), *Základné práva: výzvy a úspechy v roku 2010*, výročná správa za rok 2010, s. 59; FRA (2010), *Ochrana údajov v Európskej únii: úloha vnútroštátnych orgánov na ochranu údajov*, máj 2010.

498 SDEÚ, C-518/07, *Európska komisia/Spolková republika Nemecko* [VK], 9. marca 2010, bod 27.

499 Tamže, body 17 a 29.

500 Tamže, bod 23.

501 Tamže, bod 25.

Príklad: Vo veci *Európska Komisia/Rakúska republika*⁵⁰² SDEÚ poukázal na podobné problémy týkajúce sa postavenia určitých členov a zamestnancov rakúskeho úradu pre ochranu údajov (Komisia pre ochranu údajov, DSK). SDEÚ dospel k záveru, že skutočnosť, že spolková kancelária poskytovala dozornému orgánu svojich zamestnancov, podkopala požiadavku nezávislosti stanovenú v právnych predpisoch EÚ o ochrane údajov. SDEÚ takisto skonštatoval, že požiadavka poskytovať spolkovej kancelárii nepretržité informácie o činnosti znemožňuje úplnú nezávislosť dozorného orgánu.

Príklad: Vo veci *Európska Komisia/Maďarsko*⁵⁰³ boli podobné vnútroštátne postupy ovplyvňujúce nezávislosť zamestnancov zakázané. SDEÚ poukázal na to, že „požiadavka zabezpečiť, aby každý dozorný orgán vykonával s úplnou nezávislosťou úlohy, ktoré sú mu zverené [...] zahŕňa povinnosť dotknutého členského štátu rešpektovať dĺžku funkčného obdobia tohto orgánu tak, ako bola pôvodne stanovená“. SDEÚ ďalej rozhodol, že „Maďarsko si predčasným ukončením funkčného obdobia dozorného orgánu pre ochranu osobných údajov nespĺnilo povinnosti, ktoré mu vyplývajú zo smernice Európskeho parlamentu a Rady 95/46/ES [...]“.

Pojem „úplná nezávislosť“ a jeho kritériá sú teraz výslovne uvedené v GDPR, v ktorom sú zahrnuté zásady stanovené v uvedených rozsudkoch SDEÚ. Podľa tohto nariadenia úplná nezávislosť pri plnení úloh a vykonávaní svojich právomocí znamená, že⁵⁰⁴:

- členovia dozorného orgánu nesmú byť pod vonkajším vplyvom, či už priamym, alebo nepriamym, a nesmú od nikoho požadovať ani prijímať pokyny,
- členovia dozorného orgánu sa zdržia akéhokoľvek konania nezlučiteľného s ich povinnosťami s cieľom zabrániť konfliktu záujmov,
- členské štáty poskytnú dozornému orgánu ľudské, technické a finančné zdroje, priestory a infraštruktúru, ktoré sú potrebné na účinné plnenie jeho úloh,
- členské štáty zabezpečia, aby si každý dozorný orgán vybral svoj vlastný personál,

502 SDEÚ, C-614/10, *Európska komisia/Rakúska republika* [VK], 16. októbra 2012, body 59 a 63.

503 SDEÚ, C-288/12, *Európska komisia/Maďarsko* [VK], 8. apríla 2014, body 50 a 67.

504 Všeobecné nariadenie o ochrane údajov, článok 52.

- finančná kontrola, ktorej každý dozorný orgán podlieha podľa vnútroštátnych právnych predpisov, nesmie ovplyvniť jeho nezávislosť. Dozorné orgány musia mať samostatné a verejné ročné rozpočty, ktoré im umožnia riadne fungovať.

Nezávislosť dozorných orgánov sa takisto považuje za základnú požiadavku v rámci právnych predpisov RE. Podľa modernizovaného Dohovoru č. 108 sa vyžaduje, aby dozorné orgány „pri plnení svojich úloh a vykonávaní svojich právomocí konali úplne nezávisle a nestranne“, a to bez toho, aby požadovali alebo prijímali pokyny⁵⁰⁵. Týmto spôsobom sa Dohovorom uznáva, že tieto orgány nemôžu účinne chrániť práva a slobody jednotlivcov v súvislosti so spracúvaním údajov, pokiaľ nevykonávajú svoje funkcie úplne nezávisle. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa stanovuje viacero prvkov, ktoré prispievajú k zabezpečeniu tejto nezávislosti. K takýmto prvkom patrí možnosť, aby dozorné orgány prijímali vlastných zamestnancov a prijímali rozhodnutia bez vonkajších vplyvov, ako aj faktory týkajúce sa trvania výkonu ich funkcií a podmienky, za ktorých môžu ukončiť vykonávanie svojej funkcie⁵⁰⁶.

5.2. Príslušnosť a právomoci

Podľa právnych predpisov EÚ sa v GDPR opisuje príslušnosť a organizačná štruktúra dozorných orgánov a stanovuje, že musia byť príslušné a mať právomoc vykonávať úlohy v súlade s nariadením.

Dozorný orgán je hlavným orgánom podľa vnútroštátnych právnych predpisov, ktorý zabezpečuje súlad s právnymi predpismi EÚ o ochrane údajov. Dozorné orgány sú poverené komplexným súborom úloh a majú právomoci nad rámec monitorovania, ktoré zahŕňajú činnosti iniciatívneho a preventívneho dohľadu. Na vykonávanie týchto úloh musia mať dozorné orgány primerané vyšetrovacie, nápravné a poradné právomoci uvedené v článkoch 57 a 58 GDPR, napríklad⁵⁰⁷:

- poskytovať prevádzkovateľom a dotknutým osobám poradenstvo vo všetkých otázkach ochrany údajov,

⁵⁰⁵ Modernizovaný Dohovor č. 108, článok 15 ods. 5.

⁵⁰⁶ Dôvodová správa k modernizovanému Dohovoru č. 108.

⁵⁰⁷ Všeobecné nariadenie o ochrane údajov, články 57 a 58. Pozri aj Dohovor č. 108, Dodatkový protokol, článok 1.

- schvaľovať štandardné zmluvné doložky, záväzné vnútropodnikové pravidlá alebo administratívne dojednania,
- vyšetriť spracovateľské operácie príslušným spôsobom zasiahnuť,
- požadovať predloženie akýchkoľvek informácií dôležitých pre dohľad nad činnosťami prevádzkovateľa,
- upozorniť alebo napomenúť prevádzkovateľov a nariadiť zaslanie oznámenia porušenia ochrany osobných údajov dotknutým osobám,
- nariadiť opravu, zablokovanie, vymazanie alebo zničenie údajov,
- nariadiť dočasný alebo trvalý zákaz spracúvania alebo uložiť správne pokuty,
- postúpiť vec súdu.

Aby dozorný orgán dokázal plniť stanovené úlohy, musí mať prístup ku všetkým osobným údajom a informáciám potrebným na prešetrenie, ako aj prístup do všetkých priestorov, v ktorých prevádzkovateľ uchováva relevantné informácie. Podľa SDEÚ sa právomoci dozorného orgánu musia vykladať široko, aby sa zabezpečila úplná účinnosť ochrany údajov v prípade dotknutých osôb v EÚ.

Príklad: V rozsudku vo veci *Schrems* sa SDEÚ zaoberal otázkou, či prenos osobných údajov do USA na základe prvej dohody o Safe Harbour medzi EÚ a USA bol v súlade s právnymi predpismi EÚ o ochrane údajov, vzhľadom na odhalenia pána Edwarda Snowdena. SDEÚ argumentoval, že vnútroštátne dozorné orgány, ktoré nezávisle monitorujú spracúvanie údajov zo strany prevádzkovateľov, môžu zabrániť prenosu osobných údajov do tretej krajiny napriek existencii rozhodnutia o primeranosti, ak existujú primerané dôkazy o tom, že v tretej krajine už nie je zaručená primeraná ochrana⁵⁰⁸.

Každý dozorný orgán má právomoc vykonávať vyšetrovacie právomoci a právomoc zasahovať na svojom území. Keďže činnosti prevádzkovateľov a sprostredkovateľov sú však často cezhraničné a spracúvanie údajov má vplyv na dotknuté osoby vo

⁵⁰⁸ SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. október 2015, body 26 – 36 a 40 – 41.

viacerých členských štátoch, vzniká otázka rozdelenia právomocí medzi jednotlivými dozornými orgánmi. SDEÚ mal príležitosť preskúmať túto otázku vo veci *Weltimmo*.

Príklad: Vo veci *Weltimmo*⁵⁰⁹ sa SDEÚ zaoberal právomocou národných dozorných orgánov riešiť záležitosti týkajúce sa organizácií, ktoré nie sú zriadené v ich jurisdikcii. *Weltimmo* bola spoločnosť zaregistrovaná na Slovensku, ktorá prevádzkuje internetovú stránku, na ktorej uverejňuje inzeráty na nehnuteľnosti nachádzajúce sa v Maďarsku. Inzerenti podali sťažnosť na maďarský dozorný orgán pre ochranu osobných údajov vo veci porušenia maďarských právnych predpisov o ochrane údajov a tento orgán uložil spoločnosti *Weltimmo* pokutu. Spoločnosť napadla pokutu na vnútroštátnych súdoch a vec bola postúpená SDEÚ, aby zistil, či smernica EÚ o ochrane údajov umožňovala dozorným orgánom členského štátu uplatňovať vnútroštátne právne predpisy v oblasti ochrany údajov na spoločnosť zaregistrovanú v inom členskom štáte.

SDEÚ vyložil článok 4 ods. 1 písm. a) smernice o ochrane údajov v tom zmysle, že umožňuje uplatnenie právnej úpravy týkajúcej sa ochrany osobných údajov iného členského štátu, ako je členský štát, v ktorom je prevádzkovateľ spracúvajúci tieto údaje registrovaný, „pokiaľ tento prevádzkovateľ na území prvého členského štátu vykonáva prostredníctvom stálej prevádzkarne hoci aj minimálnu skutočnú a efektívnu činnosť“, v kontexte ktorej sa toto spracúvanie vykonáva. SDEÚ na základe informácií, ktoré mu boli predložené, konštatoval, že *Weltimmo* vykonávala v Maďarsku skutočnú a efektívnu činnosť, keďže spoločnosť mala v Maďarsku zástupcu zapísaného v slovenskom obchodnom registri s maďarskou adresou, ako aj maďarský bankový účet a poštovú schránku, a takisto vykonávala v Maďarsku činnosti v maďarskom jazyku. Z týchto informácií vyplývala existencia prevádzkarne a činnosť spoločnosti *Weltimmo* by preto podliehala maďarskému právu v oblasti ochrany údajov a právomoci maďarského dozorného orgánu. SDEÚ však ponechal na vnútroštátnom súde, aby overil informácie a rozhodol, či spoločnosť *Weltimmo* v skutočnosti mala v Maďarsku prevádzkareň.

Ak by vnútroštátny súd konštatoval, že *Weltimmo* mala prevádzkareň v Maďarsku, maďarský dozorný orgán by mal právomoc uložiť pokutu. Ak by však vnútroštátny súd rozhodol o opaku, t. j. že *Weltimmo* nemala prevádzkareň v Maďarsku, uplatniteľným právom by bolo právo členského štátu

509 SDEÚ, C-230/14, *Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. októbra 2015.

(členských štátov), v ktorom bola spoločnosť zapísaná. V tomto prípade, keďže právomoci dozorných orgánov sa musia vykonávať v súlade s územnou zvrchovanosťou ostatných členských štátov, maďarský orgán by nemohol ukladať sankcie. Keďže smernica o ochrane údajov obsahovala povinnosť spolupráce pre dozorné orgány, maďarský orgán by však mohol požiadať slovenský orgán, aby preskúmal túto záležitosť, konštatoval porušenie slovenských právnych predpisov a uložil sankcie podľa slovenských právnych predpisov.

Prijatím GDPR sa v súčasnosti uplatňujú podrobné pravidlá týkajúce sa právomoci dozorných orgánov v cezhraničných prípadoch. Nariadením sa zriaďuje „mechanizmus jednotného kontaktného miesta“ a obsahuje ustanovenia, ktoré ustanovujú spoluprácu medzi rôznymi dozornými orgánmi. V záujme účinnej spolupráce v cezhraničných prípadoch sa podľa GDPR vyžaduje určenie vedúceho dozorného orgánu ako dozorného orgánu pre hlavnú alebo jedinú prevádzkareň prevádzkovateľa alebo sprostredkovateľa⁵¹⁰. Vedúci dozorný orgán je zodpovedný za cezhraničné prípady, je jediným partnerom prevádzkovateľa alebo sprostredkovateľa a koordinuje spoluprácu s inými dozornými orgánmi v záujme dosiahnutia konsenzu. Spolupráca zahŕňa výmenu informácií, vzájomnú pomoc pri monitorovaní a vyšetrovaní a prijímaní záväzných rozhodnutí⁵¹¹.

V právnych predpisoch RE sa uvádza príslušnosť a právomoci dozorných orgánov v článku 15 modernizovaného Dohovoru č. 108. Tieto právomoci zodpovedajú právomociam, ktoré dozorné orgány majú podľa právnych predpisov EÚ vrátane právomoci v oblasti vyšetrovania a zasahovania, právomocí vydávať rozhodnutia a ukladať správne sankcie týkajúce sa porušenia ustanovení Dohovoru a právomoci iniciovať právne kroky. Nezávislé dozorné orgány majú takisto právomoc vybavovať žiadosti a sťažnosti podané dotknutými osobami, zvyšovať informovanosť verejnosti o právnych predpisoch o ochrane údajov a poskytovať poradenstvo vnútroštátnym subjektom s rozhodovacou právomocou v súvislosti s akýmkoľvek legislatívnymi alebo administratívnymi opatreniami, ktoré sa týkajú spracúvania osobných údajov.

⁵¹⁰ Všeobecné nariadenie o ochrane údajov, článok 56 ods. 1.

⁵¹¹ Tamže, článok 60.

5.3. Spolupráca

V GDPR sa stanovuje všeobecný rámec spolupráce medzi dozornými orgánmi a konkrétnejšie pravidlá spolupráce dozorných orgánov pri cezhraničných spracovateľských činnostiach.

Podľa GDPR si dozorné orgány poskytujú vzájomnú pomoc a vymieňajú si relevantné informácie v záujme konzistentného vykonávania a uplatňovania tohto nariadenia⁵¹². Dožiadaný dozorný orgán v tomto kontexte vykonáva konzultácie, kontroly a vyšetrovania. Dozorné orgány môžu vykonávať spoločné operácie vrátane spoločných vyšetrovaní a spoločných opatrení v oblasti presadzovania práva, do ktorých sú zapojení zamestnanci všetkých dozorných orgánov⁵¹³.

V EÚ prevádzkovatelia a sprostredkovatelia čoraz viac pôsobia na nadnárodnej úrovni. Vyžaduje si to úzku spoluprácu medzi príslušnými dozornými orgánmi v členských štátoch s cieľom zabezpečiť, aby spracúvanie osobných údajov bolo v súlade s požiadavkami GDPR. V rámci mechanizmu jednotného kontaktného miesta, ak má prevádzkovateľ alebo sprostredkovateľ prevádzkarne vo viacerých členských štátoch alebo ak má len jedinú prevádzkareň, ale spracovateľské operácie podstatne ovplyvňujú dotknuté osoby vo viac ako jednom členskom štáte, dozorný orgán hlavnej (alebo jedinej) prevádzkarne je vedúcim orgánom pre cezhraničné činnosti prevádzkovateľa alebo sprostredkovateľa. Vedúce orgány majú právomoc prijať opatrenia na presadzovanie práva voči prevádzkovateľovi alebo sprostredkovateľovi. Cieľom mechanizmu jednotného kontaktného miesta je zlepšiť harmonizáciu a jednotné uplatňovanie právnych predpisov EÚ o ochrane údajov v rôznych členských štátoch. Predstavuje to výhodu aj pre podniky, pretože im stačí komunikovať iba s vedúcim orgánom a nie s viacerými dozornými orgánmi. Tým sa zvyšuje právna istota pre podniky a v praxi by to malo tiež znamenať, že rozhodnutia sa prijímajú rýchlejšie a že podniky nie sú konfrontované s rôznymi dozornými orgánmi, ktoré na ne kladú konfliktné požiadavky.

Určenie vedúceho dozorného orgánu má za následok určenie miesta, kde sa nachádza hlavná prevádzkareň podniku v EÚ. Pojem „hlavná prevádzkareň“ je vymedzený v GDPR. Pracovná skupina podľa článku 29 okrem toho vydala usmernenia k určeniu

⁵¹² Tamže, článok 61 ods. 1 – 3 a článok 62 ods. 1.

⁵¹³ Tamže, článok 62 ods. 1.

vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa, ktoré zahŕňajú kritériá na identifikáciu hlavnej prevádzkarne⁵¹⁴

Na zabezpečenie vysokej úrovne ochrany údajov v celej EÚ vedúci dozorný orgán nekoná sám. Musí spolupracovať s ostatnými dotknutými dozornými orgánmi s cieľom prijímať rozhodnutia o spracúvaní osobných údajov prevádzkovateľmi a sprostredkovateľmi s cieľom dosiahnuť konsenzus a zabezpečiť konzistentnosť. Spolupráca medzi príslušnými dozornými orgánmi zahŕňa výmenu informácií, vzájomnú pomoc pri vykonávaní spoločných vyšetrovaní a monitorovacích činností⁵¹⁵. Pri poskytovaní vzájomnej pomoci dozorné orgány musia precízne zodpovedať žiadosti o informácie iných dozorných orgánov a vykonávať opatrenia v oblasti dozoru, ako sú predchádzajúce povolenia a konzultácie s prevádzkovateľom o jeho spracovateľských činnostiach, kontroly alebo vyšetrovania. Vzájomná pomoc dozorným orgánom v iných členských štátoch sa musí poskytnúť na požiadanie bez zbytočného odkladu a najneskôr do jedného mesiaca po prijatí žiadosti⁵¹⁶.

Ak má prevádzkovateľ prevádzkarne vo viacerých členských štátoch, dozorné orgány môžu vykonávať spoločné operácie vrátane vyšetrovaní a opatrení v oblasti presadzovania, do ktorých sú zapojení zamestnanci dozorných orgánov iných členských štátov⁵¹⁷.

Spolupráca medzi rôznymi dozornými orgánmi je tiež dôležitou požiadavkou v rámci práva RE. V modernizovanom Dohovore č. 108 sa stanovuje, že dozorné orgány musia navzájom spolupracovať v rozsahu potrebnom na plnenie svojich úloh⁵¹⁸. Ide napríklad o poskytnutie akýchkoľvek relevantných a užitočných informácií a koordináciu vyšetrovaní a vykonávanie spoločných akcií⁵¹⁹.

514 Pracovná skupina zriadená podľa článku 29 (2016), *Usmernenia k určeniu vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa*, WP 244, Brusel, 13. decembra 2016, revidované 5. apríla 2017.

515 Všeobecné nariadenie o ochrane údajov, článok 60 ods. 1 – 3.

516 Tamže, článok 61 ods. 1 a 2.

517 Tamže, článok 62 ods. 1.

518 Modernizovaný Dohovor č. 108, články 16 a 17.

519 Tamže, článok 17.

5.4. Európsky výbor pre ochranu údajov

V tejto kapitole už bol opísaný význam nezávislých dozorných orgánov a hlavné právomoci, ktoré majú podľa európskych právnych predpisov o ochrane údajov. Európsky výbor pre ochranu údajov (EDPB) je ďalším dôležitým aktérom pri zabezpečovaní účinného a jednotného uplatňovania pravidiel ochrany údajov v celej EÚ.

Prostredníctvom GDPR sa zriadil Európsky výbor pre ochranu údajov ako orgán EÚ s právnou subjektivitou⁵²⁰. Je nástupcom pracovnej skupiny zriadenej podľa článku 29⁵²¹, ktorá bola zriadená v smernici o ochrane údajov s cieľom poskytovať Komisii poradenstvo v súvislosti so všetkými opatreniami EÚ, ktoré majú vplyv na práva jednotlivcov, pokiaľ ide o spracúvanie osobných údajov a súkromie, s cieľom podporiť jednotné uplatňovanie smernice a poskytovať Komisii odborné stanoviská k záležitostiam týkajúcim sa ochrany údajov. Pracovná skupina zriadená podľa článku 29 pozostávala zo zástupcov dozorných orgánov členských štátov EÚ, ako aj zástupcov Komisie a EDPS.

Podobne ako pracovná skupina pozostáva EDPB z vedúcich predstaviteľov dozorných orgánov každého členského štátu a EDPS alebo ich zástupcov⁵²². EDPS má rovnaké hlasovacie práva, s výnimkou prípadov týkajúcich sa riešenia sporov, kde môže hlasovať len o rozhodnutiach týkajúcich sa zásad a pravidiel vzťahujúcich sa na inštitúcie EÚ, ktoré svojou podstatou zodpovedajú zásadám a pravidlám GDPR. Komisia má právo zúčastňovať sa na činnostiach a zasadnutiach EDPB, nemá však hlasovacie právo⁵²³. Výbor si spomedzi svojich členov jednoduchou väčšinou volí predsedu (ktorý je poverený jeho zastúpením) a dvoch podpredsedov na päťročné funkčné obdobie. EDPB má okrem toho k dispozícii aj sekretariát, ktorý mu EDPS poskytuje s cieľom zabezpečiť výboru analytickú, administratívnu a logistickú podporu⁵²⁴.

Úlohy EDPB sú podrobne uvedené v článkoch 64, 65 a 70 GDPR a zahŕňajú komplexné úlohy, ktoré sa môžu rozdeliť na tri hlavné činnosti:

520 Všeobecné nariadenie o ochrane údajov, článok 68.

521 Podľa smernice 95/46/ES mala pracovná skupina zriadená podľa článku 29 poskytovať Komisii poradenstvo týkajúce sa všetkých opatrení EÚ, ktoré majú vplyv na práva jednotlivcov, pokiaľ ide o spracúvanie osobných údajov a súkromia, podporovať jednotné uplatňovanie smernice a poskytovať Komisii odborné stanoviská k záležitostiam týkajúcim sa ochrany údajov. Pracovná skupina zriadená podľa článku 29 pozostávala zo zástupcov dozorných orgánov členských štátov EÚ, ako aj Komisie a EDPS.

522 Všeobecné nariadenie o ochrane údajov, článok 68 ods. 3.

523 Tamže, článok 68 ods. 4 a 5.

524 Tamže, článok 73 a 75.

- **Konzistentnosť:** EDPB môže vydávať právne záväzné rozhodnutia v troch prípadoch: ak dozorný orgán vzniesol relevantnú a odôvodnenú námietku v prípadoch jednotných kontaktných miest; ak existujú protichodné názory na to, ktorý dozorný orgán je vedúci; a napokon, ak príslušný dozorný orgán nepožiadá EDPB o stanovisko alebo nepostupuje podľa stanoviska EDPB⁵²⁵. Hlavnou zodpovednosťou EDPB je zabezpečiť, aby sa GDPR jednotne uplatňovalo v celej EÚ, a zohráva kľúčovú úlohu v rámci mechanizmu konzistentnosti, ako sa uvádza v [oddiele 5.5](#).
- **Konzultácie:** Úlohy EDPB zahŕňajú poskytovanie poradenstva Komisii v súvislosti s akoukoľvek otázkou týkajúcou sa ochrany osobných údajov v Únii, ako sú zmeny GDPR, revízie právnych predpisov EÚ, ktoré sa týkajú spracúvania údajov a mohli by byť v rozpore s pravidlami EÚ na ochranu údajov, alebo vydávanie rozhodnutí Komisie o primeranosti, ktoré umožňujú prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii.
- **Usmernenie:** Výbor vydáva aj usmernenia, odporúčania a najlepšie postupy na podporu konzistentného uplatňovania nariadenia a podporuje spoluprácu a výmenu informácií medzi dozornými orgánmi. Okrem toho musí podporovať združenia prevádzkovateľov alebo sprostredkovateľov, aby vypracovali kódexy správania, ako aj zaviedli mechanizmy certifikácie a pečate ochrany údajov.

Rozhodnutia EDPB možno napadnúť na SDEÚ.

5.5. Mechanizmus konzistentnosti podľa GDPR

V GDPR sa stanovuje mechanizmus konzistentnosti s cieľom zabezpečiť, aby sa nariadenie konzistentne uplatňovalo v členských štátoch, pričom dozorné orgány spolupracujú medzi sebou a v prípade potreby s Komisiou. Mechanizmus konzistentnosti sa používa v dvoch situáciách. Prvá sa týka stanovísk EDPB v prípadoch, keď príslušný dozorný orgán zamýšľa prijať opatrenia, napríklad zoznam spracovateľských operácií, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov, alebo stanoviť štandardné zmluvné doložky. Druhá sa týka záväzných rozhodnutí EDPB týkajúcich sa dozorných orgánov v prípadoch týkajúcich sa jednotného kontaktného miesta a v prípade, že dozorný orgán nedodržiava stanovisko EDPB alebo nepožiadá EDPB o stanovisko.

⁵²⁵ Tamže, článok 65.

6

Práva dotknutých osôb a ich presadzovanie

EÚ	Zahrnuté témy	RE
Právo byť informovaný		
Všeobecné nariadenie o ochrane údajov, článok 12 SDEÚ, C-473/12, <i>Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert a i.</i> , 2013 SDEÚ, C-201/14, <i>Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.</i> , 2015	Transparentnosť informácií	Modernizovaný Dohovor č. 108, článok 8
Všeobecné nariadenie o ochrane údajov, článok 13 ods. 1 a 2 a článok 14 ods. 1 a 2	Obsah informácií	Modernizovaný Dohovor č. 108, článok 8 ods. 1
Všeobecné nariadenie o ochrane údajov, článok 13 ods. 1 a článok 14 ods. 3	Čas poskytovania informácií	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. b)
Všeobecné nariadenie o ochrane údajov, článok 12 ods. 1, 5 a 7	Spôsob poskytovania informácií	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. b)
Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. d), článok 14 ods. 2 písm. e), články 77, 78 a 79	Právo na podanie sťažnosti	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. f)

EÚ	Zahrnuté témy	RE
Právo na prístup		
Všeobecné nariadenie o ochrane údajov, článok 15 ods. 1 SDEÚ, C-553/07, <i>College van burgemeester en wethouders van Rotterdam/M. E. Rijkeboer</i> , 2009. SDEÚ, spojené veci C-141/12 a C-372/12, <i>YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S</i> , 2014 SDEÚ, C-434/16, <i>Peter Nowak/Data Protection Commissioner</i> , 2017	Právo na prístup k vlastným údajom	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. b) ESLP, <i>Leander/Švédsko</i> , č. 9248/81, 1987
Právo na opravu		
Všeobecné nariadenie o ochrane údajov, článok 16	Oprava nesprávnych osobných údajov	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. e) ESLP, <i>Cemalettin Canli/Turecko</i> , č. 22427/04, 2008 ESLP, <i>Ciubotaru/Moldavsko</i> , č. 27138/04, 2010
Právo na vymazanie		
Všeobecné nariadenie o ochrane údajov, článok 17 ods. 1	Vymazanie osobných údajov	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. e) ESLP, <i>Segerstedt-Wiberg a i./Švédsko</i> , č. 62332/00, 2006
SDEÚ, C-131/12, <i>Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González [VK]</i> , 2014 SDEÚ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni</i> , 2017	Právo na zabudnutie	
Právo na obmedzenie spracúvania		
Všeobecné nariadenie o ochrane údajov, článok 18 ods. 1	Právo na obmedzenie používania osobných údajov	
Všeobecné nariadenie o ochrane údajov, článok 19	Oznamovacia povinnosť	

EÚ	Zahrnuté témy	RE
Právo na prenosnosť údajov		
Všeobecné nariadenie o ochrane údajov, článok 20	Právo na prenosnosť údajov	
Právo namietať		
Všeobecné nariadenie o ochrane údajov, článok 21 ods. 1 SDEÚ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni</i> , 2017	Právo namietať z dôvodu konkrétnej situácie dotknutej osoby	Odporúčanie o profilovaní, článok 5.3 Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. d)
Všeobecné nariadenie o ochrane údajov, článok 21 ods. 2	Právo namietať proti použitiu údajov na marketingové účely	Odporúčanie o priamom marketingu, článok 4.1
Všeobecné nariadenie o ochrane údajov, článok 21 ods. 5	Právo namietať automatizovanými prostriedkami	
Práva súvisiace s automatizovaným rozhodovaním a profilovaním		
Všeobecné nariadenie o ochrane údajov, článok 22	Práva súvisiace s automatizovaným rozhodovaním a profilovaním	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. a)
Všeobecné nariadenie o ochrane údajov, článok 21	Práva namietať voči automatizovanému rozhodovaniu	
Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. f)	Práva na zmysluplné vysvetlenie	Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. c)
Prostriedky nápravy, zodpovednosť, sankcie a náhrada škody		
Charta, článok 47 SDEÚ, C-362/14, <i>Maximillian Schrems/Data Protection Commissioner</i> [VK], 2015 Všeobecné nariadenie o ochrane údajov, články 77 – 84	Prípady porušenia vnútroštátnych predpisov o ochrane údajov	ECHR, článok 13 (len pre členské štáty Rady Európy) Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. f), články 12, 15, 16 – 21 ESLP, <i>K. U./Fínsko</i> , č. 2872/02, 2008 ESLP, <i>Biriuk/Litva</i> , č. 23373/03, 2008
Nariadenie o ochrane údajov inštitúciami EÚ, články 34 a 49. SDEÚ, C-28/08 P, <i>Európska komisia/The Bavarian Lager Co. Ltd</i> [VK], 2010	Prípady porušenia právnych predpisov EÚ inštitúciami a orgánmi EÚ	

Účinnosť právnych predpisov vo všeobecnosti a konkrétne práv dotknutých osôb závisí od existencie vhodných mechanizmov na ich presadzovanie. V digitálnom veku sa spracúvanie údajov stalo všadeprítomnou súčasťou života a pre jednotlivcov je čoraz ťažšie ho pochopiť. Aby sa zmiernila nerovnováha síl medzi dotknutými osobami a prevádzkovateľmi, jednotlivci získali určité práva na výkon väčšej kontroly nad spracúvaním svojich osobných informácií. Právo na prístup k vlastným údajom a právo na ich opravu sú zakotvené v článku 8 ods. 2 Charty, čo je dokument, ktorý je súčasťou primárneho práva EÚ a má v právnom poriadku EÚ základné postavenie. V sekundárnom práve EÚ – najmä vo všeobecnom nariadení o ochrane údajov – sa zaviedol ucelený právny rámec, ktorý posilňuje postavenie dotknutých osôb tým, že im poskytuje práva vo vzťahu k prevádzkovateľom. Okrem práva na prístup a opravu sa v GDPR vymedzuje súbor ďalších práv, ako je právo na vymazanie („právo na zabudnutie“), právo namietat alebo obmedziť spracúvanie údajov a práva súvisiace s automatizovaným rozhodovaním a profilovaním. Podobné záruky, ktoré umožnia dotknutým osobám vykonávať účinnú kontrolu nad svojimi údajmi, sú zahrnuté aj v modernizovanom Dohovore č. 108. V článku 9 sa uvádza zoznam práv, ktoré by jednotlivci mali mať možnosť využívať pri spracúvaní svojich osobných údajov. Zmluvné strany musia zabezpečiť, aby boli tieto práva k dispozícii všetkým dotknutým osobám v rámci ich jurisdikcie a aby ich sprevádzali účinné právne a praktické prostriedky, ktoré dotknutým osobám umožňujú ich vykonávanie.

Okrem toho, že sa jednotlivcom poskytujú práva, je rovnako dôležité vytvoriť mechanizmy, ktoré umožnia dotknutým osobám napadnúť porušovanie ich práv, vyvodiť zodpovednosť voči prevádzkovateľom a žiadať o náhradu škody. Právo na účinný prostriedok nápravy, ako sa zaručuje podľa ECHR a Charty, si vyžaduje, aby sa všetkým osobám poskytli súdne prostriedky nápravy.

6.1. Práva dotknutých osôb

Hlavné body

- Každá dotknutá osoba má právo na informácie o každom spracúvaní osobných údajov zo strany prevádzkovateľa, s výhradou vymedzených výnimiek.
- Dotknuté osoby majú právo:
 - na prístup k svojim vlastným údajom a získať určité informácie o spracúvaní,
 - na opravu svojich údajov prevádzkovateľom, ktorý spracúva ich údaje, ak sú údaje nesprávne,

- na to, aby prevádzkovateľ ich údaje prípadne vymazal, ak ich spracúva nezákonne,
- dočasne obmedziť spracúvanie,
- za určitých podmienok na prenosnosť svojich údajov inému prevádzkovateľovi.
- Okrem toho majú dotknuté osoby právo namietať proti spracúvaniu:
 - z dôvodov týkajúcich sa ich konkrétnej situácie,
 - pri používaní ich údajov na účely priameho marketingu.
- Dotknuté osoby majú právo na to, aby sa na ne nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní vrátane profilovania a ktoré má právne účinky, ktoré ich významne ovplyvňujú. Dotknuté osoby majú takisto právo:
 - na ľudský zásah zo strany prevádzkovateľa,
 - vyjadriť svoje stanovisko a právo napadnúť rozhodnutie na základe automatizovaného spracúvania.

6.1.1. Právo byť informovaný

Podľa **právnych predpisov RE**, ako aj **právnych predpisov EÚ** sú prevádzkovatelia spracovateľských operácií povinní informovať dotknutú osobu v čase získavania osobných údajov o ich plánovanom spracúvaní. Táto povinnosť nezávisí od žiadosti dotknutej osoby, prevádzkovateľ musí túto povinnosť iniciatívne splniť bez ohľadu na to, či dotknutá osoba prejavuje záujem o tieto informácie alebo nie.

Podľa právnych predpisov RE podľa článku 8 modernizovaného Dohovoru č. 108 zmluvné strany musia stanoviť, že prevádzkovatelia informujú dotknuté osoby o ich totožnosti a obvyklom pobyte, o právnom základe a účele spracúvania, o kategóriách spracúvaných osobných údajov, o príjemcoch ich osobných údajov (ak existujú) a o tom, ako si môžu uplatniť svoje práva podľa článku 9, čo zahŕňa právo na prístup, opravu a právne prostriedky nápravy. Dotknutým osobám by sa takisto mali oznamovať akékoľvek ďalšie doplňujúce informácie, ktoré sa považujú za potrebné na zabezpečenie spravodlivého a transparentného spracúvania osobných údajov. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa objasňuje, že informácie poskytované dotknutým osobám „by mali byť ľahko dostupné, čitateľné, zrozumiteľné a prispôbené pre konkrétne dotknuté osoby“⁵²⁶.

526 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 68.

Podľa právnych predpisov EÚ sa v súlade so zásadou transparentnosti vyžaduje, aby každé spracúvanie osobných údajov bolo vo všeobecnosti transparentné pre jednotlivcov. Jednotlivci majú právo vedieť, ako a ktoré osobné údaje sa získavajú, používajú alebo inak spracúvajú, ako aj mať informácie o rizikách, zárukách a svojich právach týkajúcich sa spracúvania⁵²⁷. V článku 12 GDPR sa tak stanovuje široká komplexná povinnosť prevádzkovateľov poskytovať transparentné informácie a/alebo informovať o tom, ako môžu dotknuté osoby uplatňovať svoje práva⁵²⁸. Informácie musia byť stručné, transparentné, zrozumiteľné a ľahko dostupné, musia byť formulované jasne a jednoducho. Musia sa predložiť v písomnej forme, v prípade potreby aj elektronicky, a môžu sa na žiadosť dotknutej osoby poskytnúť aj ústne, ak je nepochybne preukázaná jej totožnosť. Informácie sa poskytujú bez zbytočného odkladu alebo výdavkov⁵²⁹.

Článok 13 a článok 14 GDPR sa týkajú práva dotknutých osôb na informácie buď v situáciách, keď boli osobné údaje získané priamo od nich, alebo v situáciách, keď údaje neboli získané od nich.

Rozsah práva na informácie a jeho obmedzenia podľa právnych predpisov EÚ boli vysvetlené v judikatúre SDEÚ.

Príklad: Vo veci *Institut professionnel des agents immobiliers (IPI)/Englebert*⁵³⁰ bol SDEÚ požiadaný o výklad článku 13 ods. 1 smernice 95/46. V tomto článku sa členským štátom dávala možnosť prijať legislatívne opatrenia na obmedzenie rozsahu práva dotknutej osoby na informácie, ak je to potrebné na ochranu, okrem iného, práv a slobôd iných a na prevenciu a vyšetrovanie trestných činov alebo porušení etiky v prípade regulovaných povolání. IPI je profesijná organizácia realitných maklérov v Belgicku, ktorá je zodpovedná za zabezpečenie riadneho výkonu povolania realitného makléra. IPI požiadala vnútroštátny súd, aby konštatoval, že žalované osoby porušili pravidlá výkonu tohto povolania, a nariadil im, aby ukončili rôzne činnosti v oblasti obchodovania s nehnuteľnosťami. Táto žaloba sa opierala o dôkazy, ktoré predložili súkromní detektívi, na ktorých sa IPI obrátila.

527 Všeobecné nariadenie o ochrane údajov, odôvodnenie 39.

528 Tamže, článok 13 a 14; modernizovaný Dohovor č. 108, článok 8 ods. 1 písm. b).

529 Všeobecné nariadenie o ochrane údajov, článok 12 ods. 5; modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. b).

530 SDEÚ, C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert a i.*, 7. novembra 2013.

Vnútroštátny súd mal pochybnosti, pokiaľ ide o hodnotu dôkazov od detektívov, vzhľadom na možnosť, že boli získané bez dodržania požiadaviek na ochranu údajov vyplývajúcich z belgických právnych predpisov, najmä povinnosti informovať dotknuté osoby o spracúvaní ich osobných údajov pred získaním týchto informácií. SDEÚ konštatoval, že v článku 13 ods. 1 sa uvádza, že členské štáty „môžu“, ale nemajú povinnosť stanoviť vo svojich vnútroštátnych právnych predpisoch výnimky z povinnosti informovať dotknuté osoby o spracúvaní ich údajov. Keďže článok 13 ods. 1 zahŕňa predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie a stíhanie alebo porušenie etiky ako dôvody, na základe ktorých môžu členské štáty obmedziť práva jednotlivcov, mohla by sa činnosť organizácie, akou je IPI, zakladať na tomto ustanovení a súkromní detektívi konajúci v jej mene by sa naň mohli odvolávať. Ak však členský štát takúto výnimku nestanovil, dotknuté osoby musia byť informované.

Príklad: Vo veci *Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*⁵³¹ SDEÚ objasnil, či právo Únie bráni národnému orgánu verejnej správy v tom, aby preniesol osobné údaje inému orgánu verejnej správy na ich následné spracúvanie bez toho, aby dotknuté osoby boli informované o tomto prenose a spracúvaní. V danom prípade Národná agentúra pre daňovú správu neinformovala žalobcov o prenose ich údajov do Národnej zdravotnej poisťovne.

SDEÚ dospel k záveru, že požiadavka podľa práva EÚ na informovanie dotknutej osoby o spracúvaní jej osobných údajov je „o to dôležitejšia, že podmieňuje výkon práva týchto osôb na prístup k spracovávaným údajom a ich opravu [...] a ich práva na vznesenie námietok so spracovaním týchto údajov“. Zásada spravodlivého spracúvania si vyžaduje informovanie dotknutých osôb o prenose ich údajov inému orgánu verejnej moci s cieľom ich ďalšieho spracúvania. Podľa článku 13 ods. 1 smernice 95/46 členské štáty môžu obmedziť právo na informácie, ak sa to považuje za nevyhnutné na zabezpečenie dôležitého hospodárskeho záujmu štátu vrátane daňových záležitostí. Takéto obmedzenia však musia byť uložené prostredníctvom legislatívnych opatrení. Keďže ani vymedzenie údajov, ktoré sa majú previesť, ani podrobné podmienky prevodu neboli stanovené v legislatívnom opatrení, ale len v protokole medzi dvoma orgánmi verejnej moci, podmienky výnimky podľa

531 SDEÚ, C-201/14, *Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*, 1. októbra 2015.

práva EÚ neboli splnené. Žalobcovia mali byť vopred informovaní o prenose svojich údajov do Národnej zdravotnej poisťovne a o následnom spracúvaní týchto údajov.

Obsah informácií

Podľa článku 8 ods. 1 modernizovaného Dohovoru č.108 je prevádzkovateľ povinný poskytnúť dotknutej osobe všetky informácie, ktoré zabezpečujú spravodlivé a transparentné spracúvanie osobných údajov vrátane týchto informácií:

- prevádzkovateľova totožnosť a obvyklý pobyt alebo prevádzkareň,
- právny základ a účely zamýšľaného spracúvania,
- kategórie spracúvaných osobných údajov,
- príjemcovia alebo prípadné kategórie príjemcov osobných údajov,
- spôsoby, akými môžu dotknuté osoby vykonávať svoje práva.

Podľa GDPR, keď sa od dotknutej osoby získavajú osobné údaje, poskytne prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie⁵³²:

- totožnosť a kontaktné údaje prevádzkovateľa vrátane kontaktných údajov prípadnej zodpovednej osoby,
- účel a právny základ spracúvania, t. j. zmluva alebo zákonná povinnosť,
- oprávnený záujem prevádzkovateľa, ak je základom pre spracúvanie,
- prípadní príjemcovia alebo kategórie príjemcov osobných údajov,
- či budú údaje prenášané do tretej krajiny alebo medzinárodnej organizácii a či sa tento prenos zakladá na rozhodnutí o primeranosti alebo sa opiera o primerané záruky,
- doba, počas ktorej sa osobné údaje budú uchovávať, a ak jej stanovenie nie je možné, kritériá na určenie doby uchovávania údajov,

532 Všeobecné nariadenie o ochrane údajov, článok 13 ods. 1.

- práva dotknutých osôb týkajúce sa spracúvania, ako je právo na prístup k údajom, právo na ich opravu, výmaz a právo na obmedzenie spracúvania alebo právo namietať voči spracúvaniu,
- či sa poskytovanie osobných údajov vyžaduje podľa zákona alebo zmluvy, či je dotknutá osoba povinná poskytnúť svoje osobné údaje, ako aj dôsledky v prípade neposkytnutia osobných údajov,
- existencia automatizovaného rozhodovania vrátane profilovania,
- právo podať sťažnosť dozornému orgánu,
- existencia práva na odvolanie súhlasu.

V prípadoch automatizovaného rozhodovania vrátane profilovania musia dotknuté osoby dostať zmysluplné informácie o použítom postupe, ako aj význam a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

V prípadoch, keď osobné údaje nie sú priamo získané od dotknutej osoby, prevádzkovateľ ju musí o pôvode osobných údajov informovať. V každom prípade musí prevádzkovateľ informovať dotknuté osoby okrem iného aj o existencii automatizovaného rozhodovania vrátane profilovania⁵³³. Napokon, ak má prevádzkovateľ v úmysle spracúvať osobné údaje na iný účel než ten, ktorý pôvodne uviedol dotknutej osobe, podľa zásad obmedzenia účelu a transparentnosti sa vyžaduje, aby prevádzkovateľ poskytol dotknutej osobe informácie o tomto novom účele. Prevádzkovatelia musia dotknutú osobu informovať pred každým ďalším spracúvaním. Inak povedané, v prípadoch, keď dotknutá osoba poskytla súhlas so spracúvaním osobných údajov, prevádzkovateľ musí získať nový súhlas dotknutej osoby, ak sa zmení účel spracúvania údajov alebo sa doplnia ďalšie účely.

Čas poskytovania informácií

V GDPR sa rozlišuje medzi dvoma scenármi a dvoma časovými momentmi, keď prevádzkovateľ musí dotknutej osobe poskytnúť informácie:

- Ak sa osobné údaje získavajú priamo od dotknutej osoby, prevádzkovateľ musí dotknutej osobe poskytnúť všetky súvisiace informácie a informovať ju

⁵³³ Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 a článok 14 ods. 2 písm. f).

o právach podľa GDPR pri získavaní týchto údajov⁵³⁴. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel, prevádzkovateľ poskytne všetky relevantné informácie pred uskutočnením tohto spracúvania.

- Ak osobné údaje neboli získané priamo od dotknutej osoby, prevádzkovateľ je povinný poskytnúť dotknutej osobe informácie o spracúvaní „v primeranej lehote po získaní osobných údajov, najneskôr však do jedného mesiaca“, alebo pred poskytnutím údajov tretej strane⁵³⁵.

V dôvodovej správe k modernizovanému Dohovoru č. 108 sa stanovuje, že ak informovanie dotknutých osôb nie je možné v čase, keď sa začne spracúvanie, môže sa vykonať v neskoršom štádiu, napríklad keď je prevádzkovateľ z akéhokoľvek dôvodu v kontakte s dotknutou osobou⁵³⁶.

Rôzne spôsoby poskytovania informácií

Podľa právnych predpisov RE a právnych predpisov EÚ musia byť informácie, ktoré je prevádzkovateľ povinný poskytnúť dotknutým osobám, stručné, transparentné, zrozumiteľné a ľahko prístupné. Musia byť poskytnuté v písomnej forme alebo iným spôsobom vrátane elektronických prostriedkov, použitím jasného, jednoduchého a ľahko zrozumiteľného jazyka. Pri poskytovaní informácií môže prevádzkovateľ použiť štandardizované ikony na poskytnutie informácií dobre viditeľným a zrozumiteľným spôsobom⁵³⁷. Napríklad ikona predstavujúca zámok by mohla naznačovať, že údaje boli bezpečne získané a/alebo zašifrované. Dotknuté osoby môžu požiadať o ústne poskytnutie informácií. Informácie musia byť bezplatné, pokiaľ žiadosť dotknutej osoby nie je zjavne neopodstatnená alebo neprimeraná (t. j. má opakujúcu sa povahu)⁵³⁸. Ľahký prístup k poskytnutým informáciám je rozhodujúci pre schopnosť dotknutej osoby uplatňovať svoje práva stanovené v právnych predpisoch EÚ o ochrane údajov.

534 Tamže, článok 13 ods. 1 a 2, úvodná časť, kde sa vo všeobecnom nariadení o ochrane údajov odkazuje na informácie o povinnosti, ktorá sa uplatňuje „pri získavaní osobných údajov“.

535 Tamže, článok 13 ods. 3 a článok 14 ods. 3, pozri tiež odkaz na primerané intervaly a bez zbytočného odkladu podľa modernizovaného Dohovoru č. 108, článok 8 ods. 1 písm. b).

536 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 70.

537 Európska komisia ďalej vypracuje informácie, ktoré sa majú poskytovať vo forme ikon, a postupy poskytovania štandardizovaných ikon v delegovaných aktoch; pozri všeobecné nariadenie o ochrane údajov, článok 12 ods. 8.

538 Všeobecné nariadenie o ochrane údajov, článok 12 ods. 1, 5 a 7 a modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. b).

Podľa zásady spravodlivého spracúvania sa vyžaduje, aby boli informácie pre dotknuté osoby ľahko zrozumiteľné. Musí sa použiť jazyk primeraný adresátovi informácie. Úroveň a druh používaného jazyka by sa mali líšiť v závislosti od toho, či je zamýšľaným adresátom napríklad dospelý alebo dieťa, široká verejnosť alebo akademický odborník. Otázkou vyvažovania tohto aspektu zrozumiteľnosti informácií sa zaoberá stanovisko pracovnej skupiny zriadenej podľa článku 29 k harmonizovanejším ustanoveniam o poskytovaní informácií. Podporuje myšlienku tzv. viacvrstvových oznámení⁵³⁹, ktoré umožňujú dotknutej osobe rozhodnúť o tom, akú mieru podrobnosti uprednostňuje. Tento spôsob prezentácie informácií však neoslobodzuje prevádzkovateľa od jeho povinnosti podľa článku 13 a článku 14 GDPR. Prevádzkovateľ musí dotknutej osobe naďalej poskytnúť všetky informácie.

Jedným z najúčinnnejších spôsobov poskytovania informácií je uviesť príslušné ustanovenia s informáciami na domovskej stránke prevádzkovateľa, ako je politika ochrany súkromia na webovom sídle. Existuje však značná časť obyvateľstva, ktorá internet nevyužíva, a táto skutočnosť by sa mala zohľadniť v informačnej politike spoločnosti alebo orgánu verejnej moci.

Oznámenie o ochrane osobných údajov na webovej stránke v súvislosti so spracúvaním údajov by mohlo vyzeráť takto:

Kto sme?

Prevádzkovateľom pri spracúvaní údajov je spoločnosť Bed and Breakfast C&U, so sídlom v [adresa: xxx], tel: xxx; fax: xxx; e-mail info@c&u.com; kontaktné údaje zodpovednej osoby: [xxx].

Oznámenie o ochrane osobných údajoch je súčasťou podmienok upravujúcich naše hotelové služby.

Aké údaje od vás získavame?

Získavame tieto osobné údaje: vaše meno, poštová adresa, telefónne číslo, e-mailová adresa, informácie o pobyte, číslo kreditnej a platobnej karty a IP adresy alebo mená domén počítačov, ktorými ste sa pripojili na naše webové sídlo.

⁵³⁹ Pracovná skupina zriadená podľa článku 29 (2004), *Stanovisko 10/2004 ku harmonizovanejším ustanoveniam o poskytovaní informácií*, WP 100, Brusel, 25. novembra 2004.

Prečo získavame vaše údaje?

Vaše údaje spracúvame na základe vášho súhlasu a na účely vykonania rezervácie, na uzavretie a plnenie zmlúv týkajúcich sa služieb, ktoré vám ponúkame, a na splnenie požiadaviek stanovených zákonom, napríklad zákona o miestnych poplatkoch, v ktorom sa od nás vyžaduje, aby sme získavali osobné údaje s cieľom umožniť platbu mestskej dane za ubytovanie.

Ako spracúvame vaše údaje?

Vaše osobné údaje budú uchovávané počas obdobia troch mesiacov. Vaše údaje nepodliehajú postupom automatického rozhodovania.

Naša spoločnosť Bed and Breakfast C & U dodržiava prísne bezpečnostné postupy s cieľom zabezpečiť, aby vaše osobné údaje neboli poškodené, zničené alebo sprístupnené tretej strane bez vášho súhlasu a aby sa zabránilo neoprávnenému prístupu. Počítače, v ktorých sa uchovávajú informácie, sa nachádzajú v bezpečnom prostredí s obmedzeným fyzickým prístupom. Používame bezpečné firewally a iné opatrenia na obmedzenie elektronického prístupu. Ak sa údaje musia zaslať tretej strane, požadujeme, aby tretia strana mala zavedené podobné opatrenia na ochranu vašich osobných údajov.

Všetky informácie, ktoré získavame alebo zaznamenávame, sú obmedzené na naše priestory. Prístup k osobným údajom majú len osoby, ktoré potrebujú informácie na to, aby si plnili svoje povinnosti vyplývajúce z tejto zmluvy. Ak budeme potrebovať informácie na to, aby sme vás identifikovali, výslovne vás o ne požiadame. Predtým, ako vám poskytneme informácie, môžeme požadovať, aby ste sa zúčastnili našej bezpečnostnej kontroly. Osobné údaje, ktoré nám poskytnete, môžete kedykoľvek aktualizovať tým, že sa s nami priamo spojíte.

Aké sú vaše práva?

Máte právo na prístup k svojim údajom, získať kópiu vašich údajov, požiadať o ich vymazanie alebo opravu alebo požiadať o prenesenie vašich údajov inému prevádzkovateľovi.

Môžete sa nás obrátiť na adrese [info@c & U.com](mailto:info@c&u.com). Na vašu žiadosť musíme odpovedať do jedného mesiaca, ale ak je príliš zložitá alebo ak dostaneme príliš veľa ďalších žiadostí, budeme vás informovať, že táto lehota sa môže predĺžiť o ďalšie dva mesiace.

Prístup k vašim osobným údajom

Máte právo na prístup k svojim údajom a na žiadosť máte právo na informácie o dôvodoch, na základe ktorých sa spracúvajú, právo požiadať o ich vymazanie alebo opravu a právo nepodliehať čisto automatizovanému rozhodovaniu bez toho, aby sa zohľadnili vaše názory. Môžete sa nás obrátiť na adrese [info@c & U.com](mailto:info@c&u.com). Takisto máte právo namietiť proti spracúvaniu, odvolať svoj súhlas a podať sťažnosť národnému dozornému orgánu, ak sa domnievate, že toto spracúvanie údajov je v rozpore so zákonom, a máte nárok na náhradu škody spôsobenej v dôsledku nezákonného spracúvania.

Právo podať sťažnosť

Podľa GDPR sa od prevádzkovateľa vyžaduje, aby informoval dotknuté osoby o mechanizmoch v oblasti presadzovania podľa vnútroštátneho práva a práva EÚ v prípadoch porušenia ochrany osobných údajov. Prevádzkovateľ musí informovať dotknuté osoby o ich práve podať sťažnosť o porušení ochrany osobných údajov dozornému orgánu a v prípade potreby aj vnútroštátnemu súdu⁵⁴⁰. V právnych predpisoch RE sa stanovuje aj právo dotknutých osôb na informácie o prostriedkoch na uplatnenie ich práv vrátane práva na prostriedok nápravy podľa článku 9 ods. 1 písm. f).

Výnimky z povinnosti informovať

V GDPR sa stanovuje výnimka z povinnosti informovať. Podľa článku 13 ods. 4 a článku 14 ods. 5 GDPR sa povinnosť informovať dotknuté osoby neuplatňuje, ak dotknutá osoba už má všetky relevantné informácie⁵⁴¹. Okrem toho, ak osobné údaje neboli získané od dotknutej osoby, povinnosť informovať sa neuplatní, ak poskytovanie takýchto informácií nie je možné alebo je neprimerané, najmä ak sa

⁵⁴⁰ Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. d) a článok 14 ods. 2 písm. e); modernizovaný Dohovor č. 108, článok 8 ods. 1 písm. f).

⁵⁴¹ Tamže, článok 13 ods. 4 a článok 14 ods. 5 písm. a).

osobné údaje spracúvajú na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely⁵⁴².

Členské štáty majú okrem toho podľa GDPR priestor na voľné uváženie pri obmedzovaní povinnosti a práv jednotlivcov podľa nariadenia, ak ide o nevyhnutné a primerané opatrenie v demokratickej spoločnosti, napríklad s cieľom zaistiť ochranu národnej a verejnej bezpečnosti, obranu, ochranu súdnych vyšetrovaní a konaní alebo ochranu hospodárskych a finančných záujmov, ako aj súkromných záujmov, ktoré sú naliehavejšie ako záujmy ochrany údajov⁵⁴³.

Všetky výnimky alebo obmedzenia musia byť nevyhnutné v demokratickej spoločnosti a primerané sledovanému cieľu. Vo veľmi výnimočných prípadoch, napríklad zo zdravotných dôvodov, si samotná ochrana dotknutej osoby môže vyžadovať obmedzenie transparentnosti; týka sa to predovšetkým obmedzenia práva prístupu každej dotknutej osoby⁵⁴⁴. Minimálny stupeň ochrany podľa vnútroštátneho práva však musí rešpektovať podstatu základných práv a slobôd chránených právom Únie⁵⁴⁵. Vyžaduje si to, aby vnútroštátne právo obsahovalo osobitné ustanovenia, ktoré objasňujú účel spracúvania, kategórie zahrnutých osobných údajov, záruky a iné procedurálne požiadavky⁵⁴⁶.

Ak sa údaje zbierajú na účely vedeckého alebo historického výskumu, na štatistické účely alebo na účely archivácie vo verejnom záujme, v práve Únie alebo v práve členských štátov sa môžu stanoviť odchýlky od povinnosti informovať, ak je pravdepodobné, že znemožní alebo závažným spôsobom sťaží dosiahnutie týchto účelov⁵⁴⁷.

Podobné obmedzenia existujú v rámci právnych predpisov RE, keď práva udelené dotknutým osobám podľa článku 9 modernizovaného Dohovoru č. 108 môžu za prísnych podmienok podliehať možným obmedzeniam podľa článku 11 modernizovaného Dohovoru č. 108. Okrem toho, podľa článku 8 ods. 2 modernizovaného Dohovoru č. 108 sa povinnosť transparentnosti spracúvania uložená prevádzkovateľom neuplatňuje, ak dotknutá osoba už tieto informácie má.

⁵⁴² Tamže, článok 14 ods. 5 písm. b) – e).

⁵⁴³ Všeobecné nariadenie o ochrane údajov, článok 23 ods. 1.

⁵⁴⁴ Všeobecné nariadenie o ochrane údajov, článok 15.

⁵⁴⁵ Všeobecné nariadenie o ochrane údajov, článok 23 ods. 1.

⁵⁴⁶ Tamže, článok 23 ods. 2.

⁵⁴⁷ Tamže, článok 89 ods. 2 a 3.

Právo na prístup k vlastným údajom

V **právnych predpisoch RE** sa právo na prístup k vlastným údajom jednotlivca výslovne uznáva v článku 9 modernizovaného Dohovoru č. 108. Týmto sa ustanovuje, že každý jednotlivec má právo získať na požiadanie informácie o spracúvaní osobných údajov, ktoré sa ho týkajú a ktoré mu budú oznámené zrozumiteľným spôsobom. Právo na prístup bolo uznané nielen v ustanoveniach modernizovaného Dohovoru č. 108, ale aj v judikatúre ESĽP. ESĽP opakovane rozhodol, že jednotlivci majú právo na prístup k informáciám o svojich osobných údajoch a že toto právo vyplýva z potreby rešpektovať súkromný život⁵⁴⁸. Právo na prístup k osobným údajom, ktoré uchováávajú verejné alebo súkromné organizácie, však môže byť za určitých okolností obmedzené⁵⁴⁹.

Podľa právnych predpisov EÚ je právo na prístup k vlastným údajom výslovne uznané v článku 15 GDPR a takisto sa uvádza ako prvok základného práva na ochranu osobných údajov v článku 8 ods. 2 Charty⁵⁵⁰. Právo jednotlivca získať prístup k vlastným osobným údajom je kľúčovým prvkom európskeho práva v oblasti ochrany údajov⁵⁵¹.

V GDPR sa stanovuje, že každá dotknutá osoba má právo na prístup k svojim osobným údajom a určitým informáciám o spracúvaní, ktoré prevádzkovatelia musia poskytnúť⁵⁵². Každá dotknutá osoba má právo získať (od prevádzkovateľa) potvrdenie o tom, či sa spracúvajú údaje, ktoré sa jej týkajú, a aspoň tieto informácie:

- účely spracúvania,
- kategórie dotknutých osobných údajov,
- príjemcovia alebo kategórie príjemcov, ktorým boli osobné údaje poskytnuté,

548 ESĽP, *Gaskin/Spojené kráľovstvo*, č. 10454/83, 7. júla 1989; ESĽP, *Odièvre/Francúzsko* [VK], č. 42326/98, 13. februára 2003; ESĽP, *K.H. a i./Slovensko*, č. 32881/04, 28. apríla 2009; ESĽP, *Godelli/Taliano*, č. 33783/09, 25. septembra 2012.

549 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987.

550 Pozri tiež SDEÚ, spojené veci C-141/12 a C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*, 17. júla 2014; SDEÚ, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Európsky úrad pre bezpečnosť potravín (EFSA), Európska komisia*, 16. júla 2015.

551 SDEÚ, spojené veci C-141/12 a C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*, 17. júla 2014.

552 Všeobecné nariadenie o ochrane údajov, článok 15 ods. 1.

- predpokladaná doba uchovávanía osobných údajov alebo, ak to nie je možné, kritériá na jej určenie,
- existencia práva na opravu alebo vymazanie osobných údajov alebo obmedzenia ich spracúvania,
- právo podať sťažnosť dozornému orgánu,
- akékoľvek dostupné informácie o zdroji údajov, ktoré sa spracúvajú, ak sa údaje nezískali od dotknutej osoby,
- v prípade automatizovaných rozhodnutí, postup použitý pri akomkoľvek automatizovanom spracúvaní údajov.

Prevádzkovateľ musí poskytnúť dotknutej osobe kópiu spracúvaných osobných údajov. Všetky informácie poskytnuté dotknutej osobe sa musia poskytnúť v zrozumiteľnej forme, to znamená, že prevádzkovateľ musí zabezpečiť, že dotknutá osoba dokáže informácie pochopiť. Napríklad uvedenie technických skratiek, šifrovaných výrazov alebo skratiek v odpovedi na žiadosť o prístup zvyčajne nebude postačovať, pokiaľ nie je vysvetlený význam týchto pojmov. V prípade vykonávania automatizovaného rozhodovania vrátane profilovania bude potrebné vysvetliť všeobecnú logiku automatizovaného rozhodovania vrátane kritérií, ktoré boli pri hodnotení dotknutej osoby zohľadnené. Podobné požiadavky existujú v rámci **právnych predpisov RE**⁵⁵³.

Príklad: Prístup k vlastným osobným údajom pomôže dotknutej osobe určiť, či údaje sú alebo nie sú správne. Je preto nevyhnutné, aby bola dotknutá osoba informovaná v zrozumiteľnej forme nielen o samotných osobných údajoch, ktoré sa spracúvajú, ale aj o kategóriách, v rámci ktorých sa tieto osobné údaje spracúvajú, ako je meno, IP adresa, geolokalizačné súradnice, číslo kreditnej karty atď.

Ak sa údaje nezískavajú od dotknutej osoby, v odpovedi na žiadosť o prístup sa musia uviesť informácie o zdroji údajov, pokiaľ sú tieto informácie k dispozícii. Toto ustanovenie sa musí chápať v kontexte zásad spravodlivosti, transparentnosti a zodpovednosti. Prevádzkovateľ nesmie zničiť informácie o zdroji údajov s cieľom

⁵⁵³ Pozri modernizovaný Dohovor č. 108, článok 8 ods. 1 písm. c).

oslobodiť sa od povinnosti ich poskytnutia, okrem prípadu, ak by k vymazaniu došlo bez ohľadu na prijatie žiadosti o prístup, a aj tak musí prevádzkovateľ dodržať všeobecné požiadavky na „zodpovednosť“.

Ako sa uvádza v judikatúre SDEÚ, právo na prístup k osobným údajom nesmie byť neprimerane časovo obmedzené. Dotknuté osoby musia mať tiež primeranú možnosť získať informácie o spracovateľských operáciách, ktoré sa uskutočnili v minulosti.

Príklad: SDEÚ mal vo veci *Rijkeboer*⁵⁵⁴ určiť, či môže byť právo na prístup jednotlivca k informáciám o príjemcoch alebo kategóriách príjemcov osobných údajov a o obsahu oznámených údajov obmedzené na jeden rok pred podaním žiadosti o prístup.

SDEÚ rozhodol, že pri určovaní toho, či sa podľa článku 12 smernice oprávňuje na takéto časové obmedzenie, vyloží predmetný článok z hľadiska cieľov smernice. SDEÚ najprv konštatoval, že právo na prístup je nevyhnutne potrebné, aby sa dotknutej osobe umožnilo vykonať svoje právo požiadať prevádzkovateľa o opravu, vymazanie alebo zablokovanie údajov, alebo oznámenie tretím stranám, ktorým sa tieto údaje zverejnili, že došlo k úprave, vymazaniu alebo zablokovaniu. Účinné právo na prístup je takisto nevyhnutne potrebné s cieľom umožniť dotknutej osobe, aby uplatnila právo namietat' proti spracúvaniu jej osobných údajov a právo podať sťažnosť a požadovať náhradu škody⁵⁵⁵.

SDEÚ dospel k záveru, že v záujme zaistenia praktického dosahu uvedených ustanovení sa „toto právo [...] musí nevyhnutne vzťahovať na minulosť. Ak by tomu tak nebolo, dotknutá osoba by si nemohla účinne uplatniť svoje právo na vykonanie opravy, výmazu alebo zablokovania údajov, ktoré pokladá za nezákonné alebo nesprávne, ako aj na podanie súdneho prostriedku nápravy a získať náhradu za spôsobenú ujmu.“

554 SDEÚ, C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. Rijkeboer*, 7. mája 2009.

555 Všeobecné nariadenie o ochrane údajov, článok 15 ods. 1 písm. c) a f), článok 16, článok 17 ods. 2 a článok 21 a kapitola VIII.

6.1.2. Právo na opravu

Podľa právnych predpisov EÚ a RE majú dotknuté osoby právo na opravu svojich osobných údajov. Presnosť osobných údajov je nevyhnutná na zabezpečenie vysokej úrovne ochrany údajov pre dotknuté osoby⁵⁵⁶.

Príklad: Vo veci *Ciubotaru/Moldavsko*⁵⁵⁷ sťažovateľ nedokázal zmeniť záznam o svojom etnickom pôvode v úradných spisoch z moldavskej národnosti na rumunskú národnosť z toho dôvodu, že svoju žiadosť nebol schopný podložiť dôkazmi. ESLP považoval za prípustné, aby štáty požadovali objektívny dôkaz pri registrácii etnického pôvodu jednotlivca. Ak sa nárok zakladá výlučne na subjektívnych a nedoložených základoch, orgány môžu žiadosť zamietnuť. Nárok sťažovateľa však vychádzal nielen zo subjektívneho vnímania etnického pôvodu; sťažovateľ bol schopný predložiť objektívne overiteľné spojenia s rumunskou národnostnou skupinou, napríklad jazyk, meno, čítanie a iné. Podľa vnútroštátnych právnych predpisov však sťažovateľ musel predložiť dôkaz o tom, že jeho rodičia patrili k rumunskej národnostnej skupine. Vzhľadom na historické reálie Moldavska takáto požiadavka predstavovala neprekonateľnú prekážku pre registráciu inej etnickej totožnosti než tej, ktorú zapísali rodičom sťažovateľa sovietske orgány. Štát bránil sťažovateľovi v tom, aby sa jeho nárok preskúmal z hľadiska objektívne overiteľných dôkazov, čím nesplnil svoju pozitívnu povinnosť zaistiť účinné rešpektovanie súkromného života sťažovateľa. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

V niektorých prípadoch postačí, ak dotknutá osoba jednoducho požiada o opravu napríklad hláskovania mena, zmenu adresy alebo telefónneho čísla. Podľa **právnych predpisov EÚ a RE** sa nesprávne osobné údaje musia opraviť bez zbytočného alebo nadmerného oneskorenia⁵⁵⁸. Ak sa však takéto žiadosti týkajú právne významných údajov, ako je právna totožnosť dotknutej osoby alebo správne miesto pobytu na doručovanie právnych dokumentov, žiadosti o opravu nemusia byť dostatočné a prevádzkovateľ môže byť oprávnený požadovať dôkaz o tvrdenej nepresnosti údajov. Takéto požiadavky nesmú pre dotknutú osobu predstavovať nezmyselné dôkazné bremeno, a teda brániť dotknutým osobám, aby došlo k opraveniu ich

⁵⁵⁶ Tamže, článok 16 a odôvodnenie 65; modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. e).

⁵⁵⁷ ESLP, *Ciubotaru/Moldavsko*, č. 27138/04, 27. apríla 2010, body 51 a 59.

⁵⁵⁸ Všeobecné nariadenie o ochrane údajov, článok 16; modernizovaný Dohovor č. 108, článok 9 ods. 1.

údajov. ESLP zistil porušenia článku 8 ECHR vo viacerých prípadoch, v ktorých sťažovateľ nemohol napadnúť správnosť informácií uchovávaných v tajných registroch⁵⁵⁹.

Príklad: ESLP vo veci *Cemalettin Canli/Turecko*⁵⁶⁰ zistil porušenie článku 8 ECHR pri nesprávnych hláseniach polície o trestných stíhaniach.

Proti sťažovateľovi bolo dvakrát vedené trestné stíhanie za údajné členstvo v nelegálnych organizáciách, nikdy však nebol odsúdený. Keď bol znova uväznený a obžalovaný z iného trestného činu, polícia predložila trestnému súdu správu s názvom *Informačný formulár o ďalších trestných činoch*, ktorá vyvolávala dojem, že sťažovateľ je členom dvoch ilegálnych organizácií. Žiadosti sťažovateľa o zmenu správy a policajných záznamov nebolo vyhovené. ESLP potvrdil, že informácie v policajnej správe spadajú do rozsahu pôsobnosti článku 8 ECHR, pretože systematicky zbierané verejné informácie uchovávané v spisoch držaných verejnými orgánmi by takisto mohli patriť pod pojem „súkromný život“. Okrem toho bola policajná správa nesprávne vypracovaná a jej predloženie trestnému súdu nebolo v súlade s národnými právnymi predpismi. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

V priebehu občianskoprávneho konania alebo konania pred orgánom verejnej moci o správnosti údajov môže dotknutá osoba požiadať o to, aby sa v jej spise s údajmi uvádzal záznam alebo poznámka s informáciou, že ich presnosť je sporná a že sa čaká na úradné rozhodnutie⁵⁶¹. Počas tohto obdobia prevádzkovateľ nesmie prezentovať údaje ako správne alebo nepodliehajúce zmene, najmä nie tretím stranám.

6.1.3. Právo na vymazanie („právo na zabudnutie“)

Poskytnúť dotknutým osobám právo na vymazanie ich vlastných údajov je mimoriadne dôležité na účinné uplatňovanie zásad ochrany údajov, a najmä zásady minimalizácie údajov (osobné údaje sa musia obmedziť na to, čo je nevyhnutné na účely, na ktoré sa tieto údaje spracúvajú). Právo na vymazanie sa preto nachádza v právnych nástrojoch RE a EÚ⁵⁶².

⁵⁵⁹ ESLP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000.

⁵⁶⁰ ESLP, *Cemalettin Canli/Turecko*, č. 22427/04, 18. novembra 2008, body 33 a 42 – 43; ESLP, *Dalea/Francúzsko*, č. 964/07, 2. februára 2010.

⁵⁶¹ Všeobecné nariadenie o ochrane údajov, článok 18 a odôvodnenie 67.

⁵⁶² Tamže, článok 17.

Príklad: Sťažovatelia vo veci *Segerstedt-Wiberg a iní/Švédsko*⁵⁶³ boli priaznivcami určitých liberálnych a komunistických politických strán. Mali podozrenie, že informácie o nich boli zaznamenané v tajných policajných záznamoch, a požadovali ich vymazanie. EŠLP dospel k záveru, že uchovávanie predmetných údajov malo právny základ a sledoval sa ním legitímny cieľ. V prípade niektorých sťažovateľov však EŠLP konštatoval, že ďalšie uchovávanie údajov predstavuje neprimeraný zásah do ich súkromného života. Napríklad v prípade jedného zo sťažovateľov orgány uchovávali informácie o tom, že v roku 1969 sa údajne zasadzoval za násilný odpor proti policajnej kontrole počas demonstrácií. EŠLP zistil, že tieto informácie nemohli súvisieť so žiadnym relevantným bezpečnostným záujmom, predovšetkým vzhľadom na ich historickú povahu. Súd dospel k záveru, že v prípade štyroch z piatich sťažovateľov došlo k porušeniu článku 8 ECHR, keďže vzhľadom na dlhý čas, ktorý uplynul od údajných činov sťažovateľov, ďalšie uchovávanie ich údajov nebolo relevantné.

Príklad: Vo veci *Brunet/Francúzsko*⁵⁶⁴ sťažovateľ namietal voči uchovávaniu svojich osobných údajov v policajnej databáze obsahujúcej informácie o odsúdených osobách, obvinených osobách a obetiach. Napriek tomu, že trestné konanie proti sťažovateľovi bolo zastavené, jeho údaje boli zahrnuté v databáze. EŠLP dospel k záveru, že došlo k porušeniu článku 8 ECHR. Dospel aj k záveru, že sťažovateľ v praxi nemal možnosť dosiahnuť vymazanie svojich osobných údajov z databázy. EŠLP tiež posúdil povahu informácií obsiahnutých v databáze a usúdil, že dochádza k narušovaniu súkromia sťažovateľa, keďže databáza obsahuje podrobné údaje o jeho totožnosti a osobnosti. Okrem toho konštatoval, že 20-ročné obdobie uchovávania osobných záznamov v databáze je príliš dlhé, a to najmä preto, že žiadny súd sťažovateľa nikdy neodsúdil.

V modernizovanom Dohovore č. 108 sa výslovne uvádza, že každý jednotlivec má právo na vymazanie nesprávnych, nepravdivých alebo nezákonne spracúvaných údajov⁵⁶⁵.

563 EŠLP, *Segerstedt-Wiberg a i./Švédsko*, č. 62332/00, 6. júna 2006, body 89 a 90; pozri napríklad aj EŠLP, *M.K./Francúzsko*, č. 19522/09, 18. apríla 2013.

564 EŠLP, *Brunet/Francúzsko*, č. 21010/10, 18. septembra 2014.

565 Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. e).

Podľa právnych predpisov EÚ sa v článku 17 GDPR stanovuje možnosť dotknutých osôb požiadať o vymazanie údajov. Právo na vymazanie osobných údajov bez zbytočného odkladu sa uplatňuje, ak:

- osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali,
- dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie vykonáva, a ak neexistuje iný právny základ na spracúvanie,
- dotknutá osoba namieta voči spracúvaniu a neprevažujú žiadne oprávnené dôvody na spracúvanie,
- osobné údaje sa spracúvali nezákonne,
- osobné údaje musia byť vymazané, aby sa splnila zákonná povinnosť podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha,
- osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti deťom podľa článku 8 GDPR⁵⁶⁶.

Dôkazné bremeno, že spracúvanie údajov je legitímne, znášajú prevádzkovatelia, keďže sú zodpovední za zákonnosť spracúvania⁵⁶⁷. Podľa zásady zodpovednosti musí byť prevádzkovateľ kedykoľvek schopný preukázať, že na jeho spracúvanie údajov existuje vhodný právny základ, inak sa spracúvanie musí zastaviť⁵⁶⁸. V GDPR sa vymedzujú výnimky z práva na zabudnutie vrátane prípadov, keď je spracúvanie osobných údajov potrebné:

- na uplatnenie práva na slobodu prejavu a na informácie,
- na splnenie zákonnej povinnosti, ktorá si vyžaduje spracúvanie podľa práva Únie alebo práva členského štátu, ktorému prevádzkovateľ podlieha, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverejnej prevádzkovateľovi,

566 Všeobecné nariadenie o ochrane údajov, článok 17 ods. 1.

567 Tamže.

568 Tamže, článok 5 ods. 2.

- z dôvodov verejného záujmu v oblasti verejného zdravia,
- na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely,
- na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov⁵⁶⁹.

SDEÚ potvrdil význam práva na vymazanie pri zabezpečovaní vysokej úrovne ochrany údajov.

Príklad: Vo veci *Google Spain*⁵⁷⁰ sa SDEÚ zaoberal tým, či bola spoločnosť Google povinná vymazať zastarané informácie týkajúce sa finančných problémov žalobcu zo svojho zoznamu výsledkov vyhľadávania. Spoločnosť Google okrem iného spochybnila svoju zodpovednosť, tvrdiac, že poskytuje len odkaz na webovú stránku editora, na ktorej sú uvedené informácie, v tomto prípade na noviny, ktoré obsahujú informáciu o platobnej neschopnosti žalobcu⁵⁷¹. Spoločnosť Google tvrdila, že žiadosť o vymazanie neaktuálnych informácií z webovej stránky by sa mala podať hostiteľovi webovej stránky a nie spoločnosti Google, ktorá jednoducho poskytuje odkaz na pôvodnú stránku. SDEÚ dospel k záveru, že spoločnosť Google sa pri vyhľadávaní informácií na webových stránkach a na internete a pri indexácii ich obsahu s cieľom poskytovať výsledky vyhľadávania stáva prevádzkovateľom, na ktorého sa vzťahujú zodpovednosti a povinnosti podľa práva EÚ.

SDEÚ objasnil, že internetové vyhľadávače a výsledky vyhľadávania obsahujúce osobné údaje môžu umožniť vytvorenie podrobného profilu jednotlivca⁵⁷². Vyhľadávače dávajú informáciám obsiahnutým v takomto zozname výsledkov charakter všadeprítomnosti. Vzhľadom na túto potenciálnu

569 Tamže, článok 17 ods. 3.

570 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, body 55 – 58.

571 Spoločnosť Google napadla uplatňovanie pravidiel EÚ na ochranu údajov aj vzhľadom na skutočnosť, že spoločnosť Google Inc. je usadená v USA a spracúvanie osobných údajov, o ktoré v tejto veci išlo, sa takisto uskutočnilo v USA. Druhý argument týkajúci sa neuplatňovania právnych predpisov EÚ o ochrane údajov v tejto veci sa opieral o skutočnosť, že vyhľadávače nemožno považovať za „prevádzkovateľov“ pokiaľ ide o údaje zobrazované v ich výsledkoch, keďže im uvedené údaje nie sú známe a nevykonávajú nad nimi kontrolu. SDEÚ zamietol obe tvrdenia, keďže konštatoval, že smernica 95/46/ES bola v tomto prípade uplatniteľná, a pokračoval v skúmaní rozsahu pôsobnosti práv, ktoré zaručuje, najmä práva na vymazanie osobných údajov.

572 Tamže, body 36, 38, 80 – 81 a 97.

závažnosť tento zásah nemôže byť odôvodnený výlučne hospodárskym záujmom poskytovateľa tohto vyhľadávača na tomto spracúvaní. Je potrebné hľadať spravodlivú rovnováhu medzi oprávneným záujmom používateľov internetu na prístupe k informáciám a základnými právami dotknutej osoby podľa článkov 7 a 8 Charty. V čoraz viac digitalizovanej spoločnosti má požiadavka, aby osobné údaje boli správne a nepresahovali to, čo je nevyhnutné (napr. v prípade verejných informácií), zásadný význam pri zabezpečovaní vysokej úrovne ochrany údajov pre jednotlivcov. „Prevádzkovateľ tohto spracovania musí v rámci svojich zodpovedností, kompetencií a možností zaručiť, že toto spracúvanie spĺňa požiadavky“ právnych predpisov EÚ, aby právne záruky v nich stanovené mohli mať plný účinok⁵⁷³. To znamená, že právo na vymazanie osobných údajov, ak je spracúvanie zastarané alebo už nie je potrebné, sa vzťahuje aj na prevádzkovateľov, ktorí preberajú tieto informácie⁵⁷⁴.

Pri posudzovaní toho, či je spoločnosť Google povinná odstrániť odkazy týkajúce sa žalobcu, SDEÚ rozhodol, že za určitých podmienok majú jednotlivci právo požiadať o vymazanie osobných údajov. Toto právo sa môže uplatniť v prípade, že informácie týkajúce sa určitej osoby sú nesprávne, neadekvátne, irelevantné alebo neprimerané na účely spracúvania údajov. SDEÚ uznal, že toto právo nie je absolútne; musí byť v rovnováhe s inými právami, najmä s ohľadom na záujem širokej verejnosti na prístup k určitým informáciám. Každá žiadosť o vymazanie sa musí posudzovať na individuálnom základe, aby sa dosiahla rovnováha medzi základnými právami na ochranu osobných údajov a súkromného života dotknutej osoby na jednej strane a oprávnenými záujmami všetkých používateľov internetu vrátane editorov na strane druhej. SDEÚ poskytol usmernenie týkajúce sa faktorov, ktoré je potrebné zvážiť pri tomto posudzovaní. Povaha predmetných informácií je mimoriadne dôležitým faktorom. Ak sa informácie týkajú súkromného života jednotlivca a neexistuje verejný záujem na dostupnosti informácií, ochrana údajov a súkromia by prevažovala nad právom širokej verejnosti na prístup k informáciám. Naopak, ak je zrejmé, že dotknutá osoba je verejne činná osoba alebo že tieto informácie sú takej povahy, ktorá by odôvodňovala,

573 Tamže, body 81 – 83.

574 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, bod 88. Pozri tiež pracovná skupina zriadená podľa článku 29 (2014), *Usmernenia o vykonávaní rozsudku Súdneho dvora Európskej únie vo veci „Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi“* C-131/12, WP 225, Brusel, 26. novembra 2014 a Odporúčanie CM/Rec 2012(3) Výboru ministrov členským štátom o ochrane ľudských práv vo vzťahu k vyhľadávacím, 4. apríla 2012.

aby sa k nim poskytol prístup širokej verejnosti, potom prevažujúci záujem verejnosti na prístupe k informáciám môže odôvodniť zásah do základných práv dotknutej osoby na ochranu údajov a súkromia.

V nadväznosti na rozsudok prijala pracovná skupina zriadená podľa článku 29 usmernenia o vykonávaní tohto rozsudku SDEÚ⁵⁷⁵. Usmernenia obsahujú zoznam spoločných kritérií, ktoré majú dozorné orgány používať pri vybavovaní sťažností týkajúcich sa žiadostí jednotlivcov o vymazanie, pričom sa v nich vysvetľuje, čo toto právo na vymazanie zahŕňa, a poskytujú sa usmernenia k hľadaniu rovnováhy medzi týmito právami. V usmerneniach sa opätovne potvrdzuje, že posúdenia sa musia vykonávať na individuálnom základe. Keďže právo na zabudnutie nie je absolútne, výsledok žiadosti sa môže líšiť v závislosti od konkrétneho prípadu. Dôkazom toho je aj judikatúra SDEÚ po vynešení rozsudku vo veci Google.

Príklad: Vo veci *Camera di Commercio di Lecce/Manni*⁵⁷⁶ mal SDEÚ za úlohu preskúmať, či má jednotlivec právo dosiahnuť po zániku svojej spoločnosti vymazanie svojich osobných údajov uverejnených vo verejnom registri spoločností. Pán Manni požiadal obchodnú komoru v Lecce, aby vymazala jeho osobné údaje z tohto registra po tom, ako zistil, že potenciálni klienti si v registri zisťovali, že bol správcom spoločnosti, na ktorú bol pred viac ako desiatimi rokmi vyhlásený konkurz. Žalobca sa domnieval, že tieto informácie môžu odradiť potenciálnych klientov.

Pri vyvažovaní práva pána Manniho na ochranu jeho osobných údajov so záujmom širokej verejnosti o prístup k informáciám SDEÚ najprv preskúmal účel verejného registra. Poukázal na skutočnosť, že zverejnenie bolo stanovené zákonom, a najmä smernicou EÚ, ktorej cieľom je uľahčiť prístup tretích strán k informáciám o spoločnostiach. Tretie strany by preto mali mať možnosť preskúmať základné dokumenty spoločnosti a iné informácie týkajúce sa spoločnosti, „najmä [údaje] o osobách, ktoré sú oprávnené zaväzovať spoločnosť“, a mali by k nim mať prístup. Účelom zverejnenia bolo tiež zaručiť

575 Pracovná skupina zriadená podľa článku 29 (2014), *Usmernenia o vykonávaní rozsudku Súdneho dvora Európskej únie vo veci „Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi“* C-131/12, WP 225, Brusel, 26. novembra 2014.

576 SDEÚ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9. marca 2017.

právnú istotu vzhľadom na intenzívnejší obchod medzi členskými štátmi tým, že sa zabezpečí, aby tretie strany mali prístup ku všetkým relevantným informáciám o spoločnostiach v celej EÚ.

SDEÚ ďalej konštatoval, že aj po uplynutí času a dokonca aj po zrušení spoločnosti často naďalej pretrvávajú práva a zákonné povinnosti týkajúce sa zrušenej spoločnosti. Spory týkajúce sa zániku môžu byť zdĺhavé a dlhé roky po zániku spoločnosti môžu vznikať otázky týkajúce sa spoločnosti, jej vedúcich pracovníkov a likvidátorov. SDEÚ rozhodol, že vzhľadom na množstvo možných scenárov a rozdiely v premlčacích lehotách stanovených v jednotlivých členských štátoch „sa za súčasného stavu nejaví ako možné stanoviť jednotnú lehotu, ktorá začína plynúť zrušením spoločnosti a po jej uplynutí by už nebolo potrebné zapísanie a zverejnenie uvedených údajov v registri.“ Vzhľadom na legitímny cieľ zverejnenia a ťažkosti pri stanovení obdobia, na konci ktorého by sa mohli osobné údaje z registra vymazať bez toho, aby sa poškodili záujmy tretích strán, SDEÚ konštatoval, že pravidlá EÚ na ochranu údajov nezaručujú právo na vymazanie osobných údajov osôb, ktoré sa nachádzajú v situácii, v akej sa nachádza pán Manni.

Ak prevádzkovateľ zverejnil osobné údaje a je povinný tieto informácie vymazať, prevádzkovateľ je povinný a musí prijať „primerané“ kroky na informovanie ostatných prevádzkovateľov, ktorí spracúvajú tie isté údaje, o žiadosti dotknutej osoby o vymazanie. Pri činnostiach prevádzkovateľa sa musia zohľadniť dostupné technológie a náklady na vykonanie⁵⁷⁷.

6.1.4. Právo na obmedzenie spracúvania

Podľa článku 18 GDPR sa dotknutým osobám umožňuje dočasne obmedziť spracúvanie ich osobných údajov. Dotknuté osoby môžu prevádzkovateľa požiadať o obmedzenie spracúvania, ak:

- bola napadnutá správnosť osobných údajov,
- spracúvanie je protizákonné a dotknutá osoba žiada namiesto vymazania údajov obmedzenie ich použitia,

⁵⁷⁷ Všeobecné nariadenie o ochrane údajov, článok 17 ods. 2 a odôvodnenie 66.

- údaje sa musia uchovávať na účely uplatňovania alebo obhajovania právnych nárokov,
- čaká sa na rozhodnutie, či oprávnené záujmy na strane prevádzkovateľa prevážujú nad oprávnenými záujmami dotknutej osoby⁵⁷⁸.

Metódy, ktorými môže prevádzkovateľ obmedziť spracúvanie osobných údajov, by napríklad mohli zahŕňať dočasné presunutie vybraných údajov do iného systému spracúvania, zamedzenie prístupu používateľov k vybraným osobným údajom alebo dočasné odstránenie osobných údajov⁵⁷⁹. Prevádzkovateľ informuje dotknutú osobu pred tým, ako bude obmedzenie spracúvania zrušené⁵⁸⁰.

Povinnosť informovať o oprave alebo vymazaní osobných údajov alebo obmedzení spracúvania

Prevádzkovateľ oznámi každému príjemcovi, ktorému boli osobné údaje poskytnuté, každú opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania, pokiaľ sa to neukáže ako nemožné alebo si to nevyžaduje neprimerané úsilie⁵⁸¹. Ak dotknutá osoba požaduje informácie o týchto príjemcoch, prevádzkovateľ jej ich musí poskytnúť⁵⁸².

6.1.5. Právo na prenosnosť údajov

Podľa GDPR majú dotknuté osoby právo na prenosnosť údajov v situáciách, keď sa osobné údaje, ktoré poskytli prevádzkovateľovi, spracúvajú automatizovanými prostriedkami na základe súhlasu alebo ak spracúvanie osobných údajov je potrebné na plnenie zmluvy a vykonáva sa automatizovanými prostriedkami. To znamená, že právo na prenosnosť údajov sa neuplatňuje v situáciách, keď spracúvanie osobných údajov vychádza z iného právneho základu ako je súhlas alebo zmluva⁵⁸³.

Ak sa uplatňuje právo na prenosnosť údajov, dotknuté osoby majú právo na prenesenie svojich osobných údajov priamo od jedného prevádzkovateľa k druhému,

578 Tamže, článok 18 ods. 1.

579 Tamže, odôvodnenie 67.

580 Tamže, článok 18 ods. 3.

581 Tamže, článok 19.

582 Tamže.

583 Tamže, odôvodnenie 68 a článok 20 ods. 1.

ak je to technicky možné⁵⁸⁴. Na tento účel by mal prevádzkovateľ vyvinúť interoperabilné formáty, ktoré dotknutým osobám umožnia prenosnosť údajov⁵⁸⁵. V GDPR sa uvádza, že tieto formáty musia byť štruktúrované, bežne používané a strojovo čitateľné na uľahčenie interoperability⁵⁸⁶. Interoperabilita sa môže definovať v širšom zmysle ako schopnosť informačných systémov vymieňať si údaje a umožniť výmenu informácií⁵⁸⁷. Zatiaľ čo účelom používaných formátov je dosiahnutie interoperability, v GDPR sa neuvádzajú konkrétne odporúčania v súvislosti s formátom poskytovania: formáty sa budú medzi jednotlivými odvetviami líšiť⁵⁸⁸.

Podľa usmernení pracovnej skupiny zriadenej podľa článku 29 právo na prenosnosť údajov „dáva používateľom možnosť výberu, kontrolu a posilňuje ich postavenie“ s cieľom poskytnúť dotknutým osobám kontrolu nad ich vlastnými osobnými údajmi⁵⁸⁹. V týchto usmerneniach sa objasňujú hlavné prvky prenosnosti údajov, ktoré zahŕňajú:

- právo dotknutých osôb získať vlastné osobné údaje spracúvané prevádzkovateľom v štruktúrovanom, bežne používanom, strojovo čitateľnom a interoperabilnom formáte,
- právo na prenosnosť osobných údajov od jedného prevádzkovateľa druhému bez prekážok, ak je to technicky možné,
- režim kontroly – ak prevádzkovateľ odpovedá na žiadosť o uplatnenie práva na prenosnosť údajov, koná podľa pokynov dotknutej osoby, to znamená, že nie je zodpovedný za dodržiavanie práva v oblasti ochrany osobných údajov zo strany príjemcu vzhľadom na to, že dotknutá osoba rozhodne, komu sa údaje prenášajú,
- uplatnenie práva na prenosnosť údajov bez toho, aby tým bolo dotknuté akékoľvek iné právo, ako je to aj v prípade všetkých ostatných práv podľa GDPR.

584 Tamže, článok 20 ods. 2.

585 Tamže, odôvodnenie 68 a článok 20 ods. 1.

586 Tamže, odôvodnenie 68.

587 Európska komisia, oznámenie s názvom Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť, COM(2016) 205 final, 2. apríla 2016.

588 Pracovná skupina zriadená podľa článku 29 (2016), *Usmernenia k právu na prenosnosť údajov*, WP 242, 13. decembra 2016 a revidované 5. apríla 2017, s. 13.

589 Tamže.

6.1.6. Právo namietat'

Dotknuté osoby sa môžu odvolávať na svoje právo namietat' proti spracúvaniu osobných údajov z dôvodov týkajúcich sa ich konkrétnej situácie a vo vzťahu k údajom spracúvaným na účely priameho marketingu. Právo namietat' možno uplatniť automatizovanými prostriedkami.

Právo namietat' z dôvodov týkajúcich sa konkrétnej situácie dotknutých osôb

Dotknuté osoby nemajú všeobecné právo namietat' proti spracúvaniu svojich údajov⁵⁹⁰. V článku 21 ods. 1 GDPR sa dotknutým osobám udeľuje právomoc namietat' z dôvodov týkajúcich sa ich konkrétnej situácie, ak je právnym základom na spracúvanie plnenie úlohy prevádzkovateľa vo verejnom záujme alebo ak je spracúvanie založené na oprávnených záujmoch prevádzkovateľa⁵⁹¹. Právo namietat' sa vzťahuje na činnosti profilovania. Podobné právo bolo uznané v modernizovanom Dohovore č. 108⁵⁹².

Právo namietat' z dôvodov týkajúcich sa konkrétnej situácie dotknutej osoby má za cieľ dosiahnuť správnu rovnováhu medzi právami dotknutej osoby na ochranu údajov a oprávnenými právami iných subjektov pri spracúvaní ich údajov. SDEÚ však objasnil, že práva dotknutej osoby „vo všeobecnosti“ prevažujú nad hospodárskymi záujmami prevádzkovateľa údajov v závislosti od „od povahy dotknutej informácie a od jej citlivosti pre súkromný život údajového subjektu, ako aj od záujmu verejnosti disponovať touto informáciou“⁵⁹³. Podľa GDPR dôkazné bremeno znášajú prevádzkovatelia, ktorí musia predložiť presvedčivé dôvody na pokračovanie v spracúvaní⁵⁹⁴. Podobne sa v dôvodovej správe k modernizovanému Dohovoru č. 108 objasňuje, že legitímne dôvody na spracúvanie údajov (ktoré môžu mať prednosť pred právom dotknutých osôb namietat') sa musia v jednotlivých prípadoch preukázať⁵⁹⁵.

590 Pozri tiež ESĽP, *M.S./Švédsko*, č. 20837/92, 27. augusta 1997 (v tomto prípade boli zdravotné údaje oznámené bez súhlasu a bez možnosti namietat'); ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987; ESĽP, *Mosley/Spojené kráľovstvo*, č. 48009/08, 10. mája 2011.

591 Všeobecné nariadenie o ochrane údajov, odôvodnenie 69, článok 6 ods. 1 písm. e) a f).

592 Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. d); odporúčanie o profilovaní, článok 5 ods. 3.

593 SDEÚ, C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014, bod 81.

594 Pozri aj modernizovaný Dohovor č. 108, článok 98 ods. 1 písm. d), v ktorom sa uvádza, že dotknutá osoba môže namietat' proti spracúvaniu svojich údajov „pokiaľ prevádzkovateľ nepreukáže oprávnené dôvody na spracúvanie, ktoré prevažujú nad jej záujmami alebo právami a základnými slobodami“.

595 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 78.

Príklad: Vo veci *Manni*⁵⁹⁶ SDEÚ rozhodol, že vzhľadom na legitímny účel zverejnenia osobných údajov v registri spoločností, najmä vzhľadom na potrebu chrániť záujmy tretích strán a zabezpečiť právnu istotu, pán Manni v zásade nebol oprávnený dosiahnuť vymazanie svojich osobných údajov z registra spoločností. Uznal však existenciu práva namietať proti spracúvaniu tým, že uviedol, že „nemožno vylúčiť, že existujú osobitné situácie, v ktorých je z prevažujúcich a legitímnych dôvodov vyplývajúcich z konkrétneho prípadu dotknutej osoby a po uplynutí dostatočne dlhej lehoty [...] výnimočne odôvodnené obmedziť prístup k jej osobným údajom zapísaným v registri na tretie osoby, ktoré preukážu osobitný záujem na nahliadnutí do týchto údajov.“

SDEÚ sa domnieval, že je zodpovednosťou vnútroštátnych súdov posúdiť každý prípad, zohľadniť všetky relevantné okolnosti jednotlivca a existenciu legitímnych a prevažujúcich dôvodov, ktoré by výnimočne mohli odôvodniť obmedzený prístup tretích strán k osobným údajom uvedeným v registroch spoločností. Objasnil však, že pokiaľ ide o pána Manniho, samotná skutočnosť, že zverejnenie jeho osobných údajov v registri údajne ovplyvnilo jeho zákazníkov, sa nemôže považovať za legitímny a prevažujúci dôvod. Potenciálni klienti pána Manniho majú oprávnený záujem na prístupe k informáciám týkajúcim sa konkurzu jeho predchádzajúcej spoločnosti.

Výsledkom úspešnej námietky je, že prevádzkovateľ už nemôže predmetné údaje spracúvať. Spracovateľské operácie vykonané na údajoch dotknutej osoby pred podaním námietky však zostanú legítimne.

Právo namietať proti spracúvaniu údajov na účely priameho marketingu

V článku 21 ods. 2 GDPR sa stanovuje osobitné právo namietať proti použitiu osobných údajov na účely priameho marketingu, čím sa bližšie objasňuje článok 13 smernice o súkromí a elektronických komunikáciách. Toto právo je stanovené aj v modernizovanom Dohovore č. 108, ako aj v odporúčaní Rady Európy o priamom marketingu⁵⁹⁷. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa vysvet-

⁵⁹⁶ SDEÚ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore Manni*, 9. marca 2017, body 47 a 60.

⁵⁹⁷ Rada Európy, Výbor ministrov (1985), Odporúčanie Rec(85)20 členským štátom o ochrane osobných údajov používaných na účely priameho marketingu, 25. októbra 1985, článok 4 ods. 1.

luje, že námietky proti spracúvaniu údajov na účely priameho marketingu by mali viesť k bezpodmienečnému vymazaniu alebo odstráneniu dotknutých osobných údajov⁵⁹⁸.

Dotknutá osoba má právo namietať proti použitiu svojich osobných údajov na účely priameho marketingu kedykoľvek a bezplatne. Dotknuté osoby musia byť o tomto práve informované jasne a oddelene od akýchkoľvek iných informácií.

Právo namietať automatizovanými prostriedkami

Ak sa osobné informácie používajú a spracúvajú na účely služieb informačnej spoločnosti, dotknutá osoba môže uplatňovať svoje právo namietať proti spracúvaniu svojich osobných údajov automatizovanými prostriedkami.

Služby informačnej spoločnosti sú vymedzené ako každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb⁵⁹⁹.

Prevádzkovatelia poskytujúci služby informačnej spoločnosti musia mať zavedené vhodné technické opatrenia a postupy na zabezpečenie toho, aby bolo možné účinne uplatňovať právo namietať pomocou automatizovaných prostriedkov⁶⁰⁰. To môže zahŕňať napríklad blokovanie súborov cookies na webových stránkach alebo vypnutie sledovania prezerania internetu.

Právo namietať proti spracúvaniu na účely vedeckého alebo historického výskumu alebo na štatistické účely

Podľa právnych predpisov EÚ by sa mal vedecký výskum vykladať široko, aby zahŕňal napríklad technický rozvoj a demonštračné činnosti, základný výskum, aplikovaný výskum a výskum financovaný zo súkromných zdrojov⁶⁰¹. Historický výskum zahŕňa aj výskum na genealogické účely, pri zohľadnení skutočnosti, že nariadenie by sa nemalo uplatňovať na zosnulé osoby⁶⁰². Štatistické účely znamenajú akékoľvek operácie získavania a spracúvania osobných údajov potrebné na štatistické

598 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 79.

599 Smernica Európskeho parlamentu a Rady 98/34/ES zmenená smernicou 98/48/ES o postupe pri poskytovaní informácií v oblasti technických noriem a predpisov, článok 1 ods. 2.

600 Všeobecné nariadenie o ochrane údajov, článok 21 ods. 5.

601 Tamže, odôvodnenie 159.

602 Tamže, odôvodnenie 160.

získovanie alebo tvorbu štatistických výsledkov⁶⁰³. Konkrétna situácia dotknutej osoby je opäť právnym základom, pokiaľ ide o právo namietať proti spracúvaniu osobných údajov na výskumné účely⁶⁰⁴. Jedinou výnimkou je potreba spracúvania na plnenie úlohy vykonávanej z dôvodov verejného záujmu. Právo na vymazanie sa však neuplatňuje, ak je spracúvanie nevyhnutné (na základe dôvodov verejného záujmu alebo bez nich) na účely vedeckého alebo historického výskumu či na štatistické účely⁶⁰⁵.

V GDPR sa porovnávajú požiadavky vedeckého, štatistického alebo historického výskumu a práva dotknutých osôb s osobitnými zárukami a výnimkami stanovenými v článku 89. V právnych predpisoch Únie alebo členského štátu sa môžu stanoviť výnimky z práva namietať, pokiaľ je pravdepodobné, že takéto právo znemožní alebo závažným spôsobom sťaží dosiahnutie výskumných účelov, a ak sú takéto výnimky potrebné na splnenie týchto účelov.

Podľa **právnych predpisov RE** sa v článku 9 ods. 2 modernizovaného Dohovoru č. 108 stanovuje, že obmedzenia práv dotknutých osôb vrátane práva namietať môžu byť stanovené v právnych predpisoch, pokiaľ ide o spracúvanie údajov na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely, ak neexistuje žiadne rozpoznateľné riziko porušenia práv a základných slobôd dotknutých osôb.

V dôvodovej správe (ods. 41) sa však tiež uznáva, že dotknuté osoby by mali mať možnosť poskytnúť súhlas aj len s určitými oblasťami výskumu alebo časťami výskumných projektov v rozsahu, v akom je to vzhľadom na zamýšľaný účel možné, a namietať v prípade, že sa domnievajú, že spracúvanie nadmerne zasahuje do ich práv a slobôd bez legitímneho dôvodu.

Inými slovami, takéto spracúvanie by sa preto považovalo za *a priori* zlučiteľné, za predpokladu, že existujú iné záruky a že operácie v zásade vylučujú akékoľvek použitie získaných informácií pri rozhodnutiach alebo opatreniach týkajúcich sa konkrétnej osoby.

⁶⁰³ Tamže, odôvodnenie 162.

⁶⁰⁴ Tamže, článok 21 ods. 6.

⁶⁰⁵ Tamže, článok 17 ods. 3 písm. d).

6.1.7. Automatizované individuálne rozhodovanie vrátane profilovania

Automatizované rozhodnutia sú rozhodnutia prijaté na základe osobných údajov spracúvaných výhradne automatickými prostriedkami bez akéhokoľvek zásahu človeka. **Podľa právnych predpisov EÚ** nesmú dotknuté osoby podliehať automatizovaným rozhodnutiam, ktoré majú právne účinky alebo podobné významné účinky. Ak je pravdepodobné, že takéto rozhodnutia budú mať významný vplyv na životy jednotlivcov, pretože súvisia napríklad s úverovou bonitou, elektronickými postupmi prijímania zamestnancov, výkonnosťou v práci alebo analýzou správania alebo spoľahlivosti, je potrebná osobitná ochrana, aby sa zabránilo negatívnym dôsledkom. Automatizované rozhodovanie zahŕňa profilovanie, ktoré pozostáva z akejkoľvek formy automatizovaného hodnotenia „osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým na analýzu alebo predvídanie aspektov súvisiacich s výkonnosťou dotknutej osoby v práci, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom“⁶⁰⁶.

Príklad: Na rýchle posúdenie úverovej bonity budúceho zákazníka agentúry úverových referencií zhromažďujú určité údaje, napríklad spôsob, akým zákazník spravoval svoje úvery a účty týkajúce sa služieb verejných služieb, údaje o predchádzajúcich adresách zákazníka, ako aj informácie z verejných zdrojov, ako sú zoznamy voličov, verejné záznamy (vrátane súdnych rozhodnutí) alebo údaje o konkurze a platobnej neschopnosti. Tieto osobné údaje sa následne vkladajú do bodovacieho algoritmu, ktorý vypočíta celkovú hodnotu predstavujúcu úverovú bonitu potenciálneho zákazníka.

Podľa pracovnej skupiny zriadenej podľa článku 29 právo na to, aby sa na dotknutú osobu nevzťahovalo rozhodnutie založené výlučne na automatizovanom spracúvaní, ktoré môže mať pre dotknutú osobu právne účinky alebo významný vplyv, predstavuje všeobecný zákaz a nevyžaduje si, aby dotknutá osoba iniciatívne namietala proti takémuto rozhodnutiu⁶⁰⁷.

606 Tamže, odôvodnenie 71, článok 4 ods. 4 a článok 22.

607 Pracovná skupina zriadená podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP 251, 3. októbra 2017, s. 15.

Podľa GDPR však automatizované rozhodovanie s právnymi účinkami alebo také, ktoré významne ovplyvňuje jednotlivcov, môže byť prijateľné, ak je to potrebné na uzatvorenie zmluvy alebo plnenie zmluvy medzi prevádzkovateľom a dotknutou osobou, alebo ak dotknutá osoba poskytla výslovný súhlas. Automatizované rozhodovanie je prijateľné aj vtedy, ak je povolené právom a ak sú práva, slobody a oprávnené záujmy dotknutej osoby náležite chránené⁶⁰⁸.

V GDPR sa takisto stanovuje, že povinnosti prevádzkovateľa, pokiaľ ide o informácie, ktoré sa majú poskytovať pri získavaní osobných údajov, musia zahŕňať informovanie dotknutých osôb o existencii automatizovaného rozhodovania vrátane profilovania⁶⁰⁹. Právo na prístup k osobným údajom, ktoré prevádzkovateľ spracúva, zostáva nedotknuté⁶¹⁰. Informácie by nemali obsahovať len skutočnosť, že profilovanie sa uskutoční, ale aj zmysluplné informácie o použitom postupe pri profilovaní, ako aj predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu⁶¹¹. Napríklad zdravotná poisťovňa, ktorá používa automatizované rozhodovanie o žiadostiach, by mala dotknutým osobám poskytovať všeobecné informácie o tom, ako algoritmus funguje a ktoré faktory algoritmus používa na výpočet ich poistného. Podobne pri uplatňovaní svojho „práva na prístup“ môžu dotknuté osoby požiadať prevádzkovateľa o informácie o existencii automatizovaného rozhodovania a zmysluplné informácie o použitom postupe⁶¹².

Cieľom informácií poskytovaných dotknutým osobám je zabezpečiť transparentnosť a umožniť dotknutým osobám, aby prípadne poskytli informovaný súhlas alebo aby dosiahli zásah človeka. Od prevádzkovateľa sa vyžaduje, aby vykonal vhodné opatrenia na ochranu práv, slobôd a oprávnených záujmov dotknutej osoby. To zahŕňa prinajmenšom právo na ľudský zásah zo strany prevádzkovateľa a možnosť dotknutej osoby vyjadriť svoje stanovisko a napadnúť rozhodnutie založené na automatizovanom spracúvaní jej osobných údajov⁶¹³.

Pracovná skupina zriadená podľa článku 29 poskytla ďalšie usmernenia týkajúce sa používania automatizovaného rozhodovania podľa GDPR⁶¹⁴.

608 Všeobecné nariadenie o ochrane údajov, článok 22 ods. 2.

609 Tamže, článok 12.

610 Tamže, článok 15.

611 Tamže, článok 13 ods. 2 písm. f).

612 Tamže, článok 15 ods. 1 písm. h).

613 Tamže, článok 22 ods. 3.

614 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP 251, 3. októbra 2017.

V práve RE majú jednotlivci právo, aby sa na ne nevzťahovalo rozhodnutie, ktoré ich významne ovplyvní a ktoré je založené výlučne na automatizovanom spracúvaní bez zohľadnenia ich názorov⁶¹⁵. Požiadavka zohľadňovať názory dotknutej osoby pri rozhodnutiach založených výlučne na automatizovanom spracúvaní znamená, že dotknutá osoba má právo napadnúť takéto rozhodnutia a mala by mať možnosť napadnúť akékoľvek nepresnosti v osobných údajoch, ktoré používa prevádzkovateľ, a spochybníť, či je akýkoľvek jej profil relevantný⁶¹⁶. Jednotlivec však nemôže toto právo uplatniť, ak je automatizované rozhodnutie povolené zákonom, ktorému prevádzkovateľ podlieha a v ktorom sa stanovujú aj vhodné opatrenia na ochranu práv, slobôd a oprávnených záujmov dotknutej osoby. Okrem toho majú dotknuté osoby právo získať na požiadanie informácie o dôvodoch, na základe ktorých bolo spracúvanie údajov vykonané⁶¹⁷. v dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza príklad bodového hodnotenia kreditného rizika. Jednotlivci by mali byť oprávnení na získanie informácií nielen o samotnom kladnom alebo zápornom rozhodnutí, ale aj o postupe, ktorý sa pri spracúvaní ich osobných údajov použil a viedol k takémuto rozhodnutiu. „Pochopenie týchto prvkov prispieva k účinnému uplatňovaniu ďalších základných záruk, ako je právo namietat' a právo podať sťažnosť príslušnému orgánu“⁶¹⁸.

Hoci odporúčanie o profilovaní nie je právne záväzné, stanovujú sa v ňom podmienky získavania a spracúvania osobných údajov v súvislosti s profilovaním⁶¹⁹. Obsahuje ustanovenia o potrebe zabezpečiť, aby bolo spracúvanie v súvislosti s profilovaním spravodlivé, zákonné, primerané a vykonávalo sa na konkrétne a legítimné účely. Obsahuje aj ustanovenia o informáciách, ktoré by prevádzkovatelia mali dotknutým osobám poskytovať. V odporúčaní sa stanovuje aj zásada kvality údajov – od prevádzkovateľov sa vyžaduje, aby prijali opatrenia na opravu faktorov nepresnosti údajov, na obmedzenie rizík alebo chýb, ktoré z profilovania môžu vyplývať, a aby pravidelne vyhodnocovali kvalitu použitých údajov a algoritmov.

615 Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. a).

616 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 75.

617 Modernizovaný Dohovor č. 108, článok 9 ods. 1 písm. c).

618 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 77.

619 Rada Európy, [Odporúčanie Rec\(2010\)13](#) Výboru ministrov členským štátom o ochrane jednotlivcov so zreteľom na automatické spracovanie osobných údajov v kontexte profilovania, 23. novembra 2010, článok 5 ods. 5.

6.2. Prostriedky nápravy, zodpovednosť, sankcie a náhrada škody

Hlavné body

- Podľa modernizovaného Dohovoru č. 108 sa vo vnútroštátnych právnych predpisoch zmluvných strán musia stanoviť primerané prostriedky nápravy a sankcie v prípade porušenia práva na ochranu údajov.
- V EÚ sa prostredníctvom GDPR ustanovujú prostriedky nápravy pre dotknuté osoby v prípadoch porušenia ich práv, ako aj sankcie voči prevádzkovateľom a sprostredkovateľom, ktorí nedodržiavajú ustanovenia nariadenia. Ustanovuje aj právo na náhradu škody a zodpovednosť.
 - Dotknuté osoby majú právo podať dozornému orgánu sťažnosť na údajné porušenie nariadenia, ako aj právo na účinný súdny prostriedok nápravy a na získanie náhrady škody.
 - Pri uplatňovaní svojho práva na účinný prostriedok nápravy môžu byť jednotlivci zastupovaní neziskovými organizáciami pôsobiacimi v oblasti ochrany údajov.
 - Prevádzkovateľ alebo sprostredkovateľ je zodpovedný za akúkoľvek majetkovú a nemajetkovú ujmu v dôsledku porušenia.
 - Dozorné orgány majú právomoc ukladať správne pokuty za porušenia nariadenia do výšky 20 000 000 EUR alebo v prípade podniku 4 % z celkového svetového ročného obratu – podľa toho, ktorá suma je vyššia.
- Dotknuté osoby sa môžu v prípade porušenia právnych predpisov o ochrane údajov obrátiť za určitých podmienok, a ako na poslednú inštanciu, na ESLP.
- Každá fyzická alebo právnická osoba má právo podať sťažnosť proti akýmkoľvek rozhodnutiam EDPB na SDEÚ za podmienok stanovených v zmluvách.

Prijatie právnych nástrojov nestačí na zabezpečenie ochrany osobných údajov v rámci Európy. Účinnosť európskych pravidiel ochrany údajov si vyžaduje vytvorenie mechanizmov, ktoré umožnia jednotlivcom bojovať proti porušovaniu ich práv a žiadať náhradu za akúkoľvek spôsobenú škodu. Je tiež dôležité, aby dozorné orgány mali právomoc ukladať sankcie, ktoré sú účinné, odradzujúce a primerané danému porušeniu právnych predpisov.

Práva vyplývajúce z právnych predpisov o ochrane údajov môže uplatňovať osoba, o ktorej práva ide; teda dotknutá osoba. Iné osoby, ktoré spĺňajú potrebné

požiadavky podľa vnútroštátneho práva, môžu tiež zastupovať dotknuté osoby pri uplatňovaní ich práv. Podľa viacerých vnútroštátnych právnych predpisov musia byť deti a osoby s mentálnym postihnutím zastúpené svojimi porúčikmi alebo opatrovníkmi⁶²⁰. Podľa právnych predpisov EÚ o ochrane údajov môže združenie, ktorého legitímnym cieľom je podporovať práva na ochranu údajov, zastupovať dotknuté osoby pred dozorným orgánom alebo pred súdom⁶²¹.

6.2.1. Právo podať sťažnosť dozornému orgánu

Podľa **právnych predpisov RE** a EÚ majú jednotlivci právo podávať žiadosti a sťažnosti príslušnému dozornému orgánu, ak sa domnievajú, že spracúvanie ich osobných údajov sa nevykonáva v súlade s právnymi predpismi.

V modernizovanom Dohovore č. 108 sa uznáva právo dotknutých osôb využívať pomoc dozorného orgánu pri uplatňovaní ich práv vyplývajúcich z Dohovoru bez ohľadu na ich štátnu príslušnosť alebo bydlisko⁶²². Žiadosť o pomoc sa môže zamietnuť len za výnimočných okolností a dotknuté osoby by nemali uhrádzať náklady a poplatky súvisiace s pomocou⁶²³.

Podobné ustanovenia možno nájsť v právnom systéme EÚ. Podľa GDPR sa od dozorných orgánov vyžaduje, aby prijali opatrenia na uľahčenie podávania sťažností, ako je vytvorenie elektronického formulára sťažnosti⁶²⁴. Dotknutá osoba môže podať sťažnosť dozornému orgánu v členskom štáte svojho obvyklého pobytu, mieste výkonu práce alebo v mieste údajného porušenia⁶²⁵. Sťažnosti sa musia preskúmať a dozorný orgán musí dotknutú osobu informovať o výsledku postupu vybavovania sťažnosti⁶²⁶.

620 FRA (2015), *Príručka o európskom práve týkajúcom sa práv dieťaťa*, Luxemburg, Úrad pre publikácie; FRA (2013), *Spôsobilosť osôb s mentálnym postihnutím a osôb s duševnými poruchami na právne úkony*, Luxemburg, Úrad pre publikácie.

621 Všeobecné nariadenie o ochrane údajov, článok 80.

622 Modernizovaný Dohovor č. 108, článok 18.

623 Tamže, články 16 – 17.

624 Všeobecné nariadenie o ochrane údajov, článok 57 ods. 2.

625 Tamže, článok 77 ods. 1.

626 Tamže, článok 77 ods. 2.

Možné porušenia právnych predpisov zo strany inštitúcií alebo orgánov EÚ možno oznámiť EDPS⁶²⁷. Ak EDPS neodpovie do šiestich mesiacov, sťažnosť treba pokladať za zamietnutú. Odvolania proti rozhodnutiam EDPS možno podať na SDEÚ v rámci nariadenia (ES) č. 45/2001, ktorým sa inštitúciám a orgánom EÚ ukladá povinnosť dodržiavať pravidlá ochrany údajov.

Musí existovať možnosť podať odvolanie na súde proti rozhodnutiam vnútroštátneho dozorného orgánu. To sa vzťahuje na dotknutú osobu, ako aj na prevádzkovateľa a sprostredkovateľa, ktorí boli účastníkmi konania pred dozorným orgánom.

Príklad: V septembri 2017 španielsky orgán pre ochranu osobných údajov uložil spoločnosti Facebook pokutu za porušenie niekoľkých ustanovení o ochrane údajov. Dozorný orgán odsúdil sociálnu sieť za získavanie, uchovávanie a spracúvanie osobných údajov vrátane osobitných kategórií osobných údajov na reklamné účely a bez súhlasu dotknutej osoby. Základom pre rozhodnutie bolo vyšetrovanie, ktoré sa uskutočnilo z vlastnej iniciatívy dozorného orgánu.

6.2.2. Právo na účinný súdny prostriedok nápravy

Okrem práva podať sťažnosť dozornému orgánu musia mať jednotlivci právo na účinný súdny prostriedok nápravy a možnosť obrátiť sa na súd. Právo na právny prostriedok nápravy je dobre zakotvené v európskej právnej tradícii a uznáva sa ako základné právo tak podľa článku 47 Charty, ako aj podľa článku 13 ECHR⁶²⁸.

Podľa právnych predpisov EÚ vyplýva dôležitosť poskytnutia účinných právnych prostriedkov nápravy dotknutým osobám v prípade porušenia ich práv z ustanovení GDPR, v ktorom sa stanovuje právo na účinný súdny prostriedok nápravy voči dozorným orgánom, prevádzkovateľom a sprostredkovateľom, a z judikatúry SDEÚ.

627 Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov, Ú. v. ES L 8, 2001.

628 Pozri napríklad ESĽP, *Karabeyoğlu/Turecko*, č. 30083/10, 7. júna 2016; ESĽP, *Mustafa Sezgin Tanrikulu/Turecko*, č. 27473/06, 18. júla 2017.

Príklad: Vo veci *Schrems*⁶²⁹ SDEÚ vyhlásil rozhodnutie o primeranosti systému Safe Harbour za neplatné. Toto rozhodnutie umožňovalo medzinárodné prenosy údajov z EÚ organizáciám v USA, ktoré osvedčili dodržiavanie zásad v rámci systému Safe Harbour. SDEÚ sa domnieval, že systém Safe Harbour má viacero nedostatkov, ktoré ohrozovali základné práva občanov EÚ na ochranu súkromia, ochranu osobných údajov a právo na účinný opravný prostriedok.

Pokiaľ ide o porušenie práv na súkromie a ochranu údajov, SDEÚ zdôraznil, že podľa právnych predpisov USA sa určitým orgánom verejnej moci povoľuje prístup k osobným údajom preneseným z členských štátov do USA a ich spracúvanie spôsobom nezlučiteľným s pôvodným účelom prenosu a nad rámec toho, čo je prísne nevyhnutné a primerané na ochranu národnej bezpečnosti. Pokiaľ ide o právo na účinný prostriedok nápravy, uviedol, že dotknuté osoby nemajú k dispozícii žiadne správne ani súdne prostriedky nápravy, ktoré by im umožnili prístup k údajom, ktoré sa ich týkajú, a ich opravu alebo vymazanie. SDEÚ dospel k záveru, že právna úprava, ktorá neposkytuje nijakú možnosť uplatniť právne prostriedky nápravy, pokiaľ ide o prístup osoby k osobným údajom, opravu alebo vymazanie takýchto údajov, „nerešpektuje podstatu obsahu základného práva na účinnú súdnu ochranu, ako je upravené článkom 47 Charty“. Zdôraznil, že samotná existencia súdneho prostriedku nápravy na účely dodržania ustanovení práva Únie je súčasťou existencie právneho štátu.

Jednotlivci, prevádzkovatelia alebo sprostredkovatelia, ktorí chcú napadnúť právne záväzné rozhodnutie dozorného orgánu, môžu podať návrh na začatie konania na súde⁶³⁰. Pojem „rozhodnutie“ by sa mal vykladať široko a vzťahovať sa na výkon vyšetrovacích, nápravných a povoľovacích právomocí dozorných orgánov, ako aj na rozhodnutia o nevyhovení alebo zamietnutí sťažnosti. Právne nezáväzné opatrenia, ako sú stanoviská alebo rady dozorného orgánu, však nemôžu byť predmetom konania na súde⁶³¹. Návrh na začatie konania sa musí podať na súdoch členského štátu, v ktorom je príslušný dozorný orgán zriadený⁶³².

629 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

630 Všeobecné nariadenie o ochrane údajov, článok 78.

631 Tamže, odôvodnenie 143.

632 Tamže, článok 78 ods. 3.

V prípadoch, keď prevádzkovateľ alebo sprostredkovateľ porušujú práva dotknutej osoby, sú dotknuté osoby oprávnené podať návrh na začatie konania na súde⁶³³. V prípade konaní začatých proti prevádzkovateľovi alebo sprostredkovateľovi je mimoriadne dôležité, aby sa jednotlivcom poskytla možnosť voľby, kam podať žalobu. Môžu tak urobiť buď v členskom štáte, v ktorom má prevádzkovateľ alebo sprostredkovateľ prevádzkareň, alebo v členskom štáte, v ktorom majú dotknuté osoby obvyklý pobyt⁶³⁴. Druhá možnosť vo veľkej miere uľahčuje jednotlivcom uplatňovanie ich práv, pretože im umožňuje podávať žaloby v štáte, v ktorom majú bydlisko, a v rámci známej jurisdikcie. Obmedzenie miesta na vedenie konania proti prevádzkovateľom a sprostredkovateľom na členský štát, v ktorom majú prevádzkovatelia prevádzkareň, by mohlo odradiť dotknuté osoby s bydliskom v inom členskom štáte od podania žaloby, keďže by to znamenalo cestovanie a dodatočné náklady, a konanie by mohlo prebiehať v cudzom jazyku a jurisdikcii. Jediná výnimka sa týka prípadov, keď prevádzkovateľ alebo sprostredkovateľ sú orgánmi verejnej moci a spracúvanie sa vykonáva v rámci výkonu verejnej moci. V takom prípade sú príslušné len súdy štátu, v ktorom sa nachádza príslušný orgán verejnej moci⁶³⁵.

Zatiaľ čo vo väčšine prípadov sa o veciach týkajúcich sa pravidiel ochrany údajov rozhodne na súdoch členských štátov, niektoré prípady sa môžu predložiť SDEÚ. Prvou možnosťou je, ak dotknutá osoba, prevádzkovateľ, sprostredkovateľ alebo dozorný orgán požiada o zrušenie rozhodnutia EDPB. Táto žaloba však podlieha podmienkam uvedeným v článku 263 ZFEÚ, to znamená, že na to, aby bola prípustná, tieto osoby a subjekty musia preukázať, že rozhodnutie EDPB sa ich priamo a osobne týka.

Druhý prípad sa týka prípadov inštitúcií alebo orgánov EÚ, ktoré nezákonne spracúvajú osobné údaje. V prípadoch, keď inštitúcie EÚ porušujú právne predpisy o ochrane údajov, môžu dotknuté osoby podať žalobu priamo na Všeobecný súd EÚ (Všeobecný súd je súčasťou SDEÚ). Všeobecný súd je v prvej inštancii zodpovedný za sťažnosti týkajúce sa porušovania práva Únie zo strany inštitúcií Únie. Na Všeobecný súd je preto možné podávať aj sťažnosti proti EDPS – ako inštitúcii EÚ⁶³⁶.

633 Tamže, článok 79.

634 Tamže, článok 79 ods. 2.

635 Tamže.

636 Nariadenie (ES) č. 45/2001, článok 32 ods. 3.

Príklad: Vo veci *Bavarian Lager*⁶³⁷ táto spoločnosť požiadala Európsku komisiu o sprístupnenie úplnej verzie zápisnice zo stretnutia, ktoré zorganizovala Komisia a ktoré sa údajne týkalo právnych otázok relevantných pre uvedenú spoločnosť. Komisia zamietla žiadosť spoločnosti o prístup k dokumentu na základe prevažujúcich záujmov ochrany údajov⁶³⁸. Spoločnosť *Bavarian Lager* podala v súlade s článkom 32 nariadenia o ochrane údajov inštitúciami EÚ sťažnosť na SDEÚ, presnejšie sa obrátila na Súd prvého stupňa (predchodcu Všeobecného súdu). Súd prvého stupňa vo svojom rozhodnutí vo veci T-194/04, *The Bavarian Lager Co. Ltd./Komisia*, zrušil rozhodnutie Komisie o zamietnutí žiadosti o prístup. Európska komisia sa proti rozsudku odvolala na SDEÚ.

Veľká komora SDEÚ vyniesla rozsudok, ktorým zrušila rozsudok Súdu prvého stupňa a potvrdila zamietnutie Európskej komisie, pokiaľ ide o žiadosť o prístup k celej zápisnici zo stretnutia, s cieľom chrániť osobné údaje účastníkov stretnutia. SDEÚ sa domnieval, že Komisia postupovala správne, keď odmietla zverejniť tieto informácie, vzhľadom na to, že účastníci nesúhlasili so zverejnením svojich osobných údajov. Okrem toho spoločnosť *Bavarian Lager* nepreukázala nevyhnutnosť prístupu k týmto informáciám.

Dotknuté osoby, dozorné orgány, prevádzkovatelia alebo sprostredkovatelia môžu v priebehu vnútroštátneho konania požiadať vnútroštátny súd, aby požiadal SDEÚ o objasnenie výkladu a platnosti aktov inštitúcií, orgánov, úradov alebo agentúr EÚ. Takéto objasnenia sa nazývajú prejudiciálne rozhodnutia. Nejde o priamy prostriedok nápravy pre sťažovateľa, vnútroštátnym súdom však umožňuje zabezpečiť, že uplatňujú správny výklad právnych predpisov EÚ. Vďaka tomuto mechanizmu prejudiciálnych rozhodnutí sa na SDEÚ dostali aj významné prípady ako *Digital Rights Ireland* a *Kärntner Landesregierung a i.*⁶³⁹, ako aj *Schrems*⁶⁴⁰ – ktoré výrazne ovplyvnili vývoj práva EÚ v oblasti ochrany údajov.

637 SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd* [VK], 2010.

638 K analýze argumentu pozri EDPS (2011), Verejný prístup k dokumentom obsahujúcim osobné údaje po vynesení rozsudku *Bavarian Lager*, Brusel, EDPS.

639 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

640 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

Príklad: Spojené veci *Digital Rights Ireland a Kärntner Landesregierung a i.*⁶⁴¹ predložili írsky High Court a rakúsky ústavný súd s otázkou súladu smernice 2006/24/ES (smernica o uchovávaní údajov) s právnymi predpismi EÚ o ochrane údajov. Rakúsky ústavný súd položil SDEÚ otázky týkajúce sa platnosti článkov 3 až 9 smernice 2006/24/ES so zreteľom na články 7, 9 a 11 Charty. Týkali sa tiež toho, či sú určité ustanovenia rakúskeho spolkového zákona o telekomunikáciách, ktorým sa transponuje smernica o uchovávaní údajov, zlučiteľné alebo nezlučiteľné s aspektmi smernice o ochrane údajov a nariadením o ochrane údajov inštitúciami EÚ.

Vo veci *Kärntner Landesregierung a i.* pán Seitlinger, jeden zo sťažovateľov v rámci konania na Ústavnom súde, tvrdil, že používa telefón, internet a e-mail na služobné účely aj v súkromnom živote. Informácie, ktoré odosiela a prijíma, teda prechádzali cez verejné telekomunikačné siete. Podľa rakúskeho zákona o telekomunikáciách z roku 2003 je jeho poskytovateľ telekomunikačných služieb zo zákona povinný získavať a uchovávať údaje o tom, ako používa sieť. Pán Seitlinger sa domnieval, že takto získavať a uchovávať osobné údaje vôbec nie je nevyhnutné na technické účely zasielania a prijímania informácií po sieti. Podobne nie je nevyhnutné získavať a uchovávať údaje na účely fakturácie. Pán Seitlinger uviedol, že určite neposkytol súhlas s takýmto používaním svojich osobných údajov a že jediným dôvodom ich získavania a uchovávaní bol rakúsky zákon o telekomunikáciách z roku 2003.

Pán Seitlinger sa preto obrátil na rakúsky ústavný súd, kde tvrdil, že zákonné povinnosti jeho poskytovateľa telekomunikačných služieb porušujú jeho základné práva vyplývajúce z článku 8 Charty. Vzhľadom na to, že rakúskymi právnymi predpismi sa uplatňovalo právo EÚ (vtedajšia smernica o uchovávaní údajov), rakúsky ústavný súd postúpil vec SDEÚ, aby rozhodol o zlučiteľnosti smernice s právami na súkromie a ochranu údajov zakotvenými v Charte.

O tomto prípade rozhodovala veľká komora SDEÚ a výsledkom bolo zrušenie smernice EÚ o uchovávaní údajov. SDEÚ konštatoval, že smernica obsahuje mimoriadne závažný zásah do základných práv na súkromie a ochranu údajov bez toho, aby sa tento zásah obmedzoval na to, čo je nevyhnutne potrebné. Smernicou sa sledoval legitímny cieľ, keďže poskytovala vnútroštátnym

641 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014.

orgánom ďalšie príležitosti na vyšetrovanie a stíhanie závažných trestných činov, a preto predstavovala cenný nástroj pri vyšetrovaní trestných činov. SDEÚ však konštatoval, že obmedzenia základných práv by sa mali uplatňovať len vtedy, ak je to nevyhnutne potrebné, a mali by sa k nim poskytnúť jasné a presné pravidlá týkajúce sa ich rozsahu spolu so zárukami pre jednotlivcov.

Podľa SDEÚ sa touto smernicou nepodarilo toto kritérium nevyhnutnosti splniť. Po prvé sa nestanovili jasné a presné pravidlá obmedzujúce rozsah zásahu. Namiesto toho, aby sa požadovala súvislosť medzi uchovávanými údajmi a závažnou trestnou činnosťou, sa smernica vzťahovala na všetky metaúdaje všetkých používateľov elektronických komunikačných prostriedkov. Predstavovala teda zásah do práva na súkromie a ochranu údajov prakticky celého obyvateľstva EÚ, čo je možné považovať za neprimerané. Smernica neobsahovala podmienky, ktorými by sa obmedzovali osoby s oprávnením na prístup k osobným údajom, a tento prístup nepodliehal ani procesným podmienkam, napríklad požiadavke získať pred prístupom súhlas správneho orgánu alebo súdu. V smernici sa napokon nestanovovali ani jasné záruky ochrany uchovávaných údajov. Nezabezpečila sa teda účinná ochrana údajov pred rizikom zneužitia a pred akýmkoľvek nezákonným prístupom a použitím údajov⁶⁴².

SDEÚ musí v zásade odpovedať na otázky, ktoré mu boli položené, a nemôže odmietnuť vydať predbežný nález s odôvodnením, že odpoveď by buď nebola relevantná, alebo by nebola vhodne načasovaná vzhľadom na pôvodný prípad. Odmietnuť otázku však môže v prípade, že otázka nepatrí do rozsahu jeho pôsobnosti⁶⁴³. SDEÚ rozhoduje len o základných prvkoch návrhu na začatie prejudiciálneho konania, zatiaľ čo vnútroštátnemu súdu naďalej prináleží rozhodovať v pôvodnej veci⁶⁴⁴.

Podľa **právnych predpisov RE** musia zmluvné strany stanoviť vhodné súdne a mimosúdne prostriedky nápravy v prípade porušenia ustanovení modernizovaného Dohovoru č. 108⁶⁴⁵. Údajné porušenia práv na ochranu údajov v rozpore s článkom 8 ECHR voči niektorej zo zmluvných strán ECHR sa po vyčerpaní všetkých dostupných

642 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014, bod 69.

643 SDEÚ, C-244/80, *Pasquale Foglia/Mariella Novello* (č. 2), 16. decembra 1981; SDEÚ, C-467/04, *Trestné konanie proti Giuseppe Francesco Gasparini a iní.*, 28. septembra 2006.

644 SDEÚ, C-438/05, *International Transport Workers' Federation a Finnish Seamen's Union/Viking Line ABP a OÜ Viking Line Eesti* [VK], 11. decembra 2007, bod 85.

645 Modernizovaný Dohovor č. 108, článok 12.

vnútroštátnych prostriedkov nápravy môžu dodatočne predložiť ESLP. Prípady týkajúce sa porušenia článku 8 ECHR predložený ESLP musí spĺňať aj ďalšie kritériá prípustnosti (články 34 – 35 ECHR)⁶⁴⁶.

Hoci sťažnosti podávané na ESLP môžu byť namierené len proti zmluvným stranám, môžu sa tiež nepriamo zaoberať konaním alebo opomenutím súkromných strán, pokiaľ zmluvná strana nespĺnila svoje pozitívne povinnosti vyplývajúce z ECHR a vo svojom vnútroštátnom práve neposkytla dostatočnú ochranu pred porušovaním práv na ochranu údajov.

Príklad: Vo veci *K.U./Fínsko*⁶⁴⁷ sa sťažovateľ – maloletá osoba – sťažoval, že v jeho mene bol na internetovej zoznamovacej stránke umiestnený inzerát sexuálnej povahy. Poskytovateľ služby odmietol odhaliť totožnosť osoby, ktorá zverejnila tieto informácie, z dôvodu povinnosti zachovávať dôvernosť podľa fínskeho práva. Sťažovateľ tvrdil, že fínske právne predpisy mu neposkytli dostatočnú ochranu pred krokmi súkromnej osoby, ktorá o ňom umiestnila na internete inkriminujúce údaje. ESLP rozhodol, že štáty nie sú len povinné zdržať sa svojvoľného zasahovania do súkromného života jednotlivcov, ale môžu tiež mať pozitívne povinnosti, ktoré zahŕňajú „prijatie opatrení, ktorých cieľom je zabezpečiť rešpektovanie súkromného života aj v oblasti vzťahov medzi jednotlivcami“. Praktická a účinná ochrana sťažovateľa si v tomto prípade vyžadovala prijatie účinných opatrení na identifikáciu a stíhanie páchatela. Štát však takúto ochranu neposkytol a súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Príklad: Sťažovateľka vo veci *Köpke/Nemecko*⁶⁴⁸ čelila podozreniu z krádeže na pracovisku, a preto bola tajne sledovaná prostredníctvom videozáznamu. ESLP dospel k záveru, že „nič nenaznačuje, že by sa domáce orgány neusilovali o dosiahnutie rovnováhy, v rámci priestoru na voľnú úvahu, medzi právom sťažovateľky na rešpektovanie jej súkromného života podľa článku 8, záujmom jej zamestnávateľa na ochrane svojich majetkových práv a verejným záujmom na presadzovaní spravodlivosti“. Sťažnosť bola teda vyhlásená za neprípustnú.

646 ECHR, články 34 – 37.

647 ESLP, *K. U./Fínsko*, č. 2872/02, 2. decembra 2008.

648 ESLP, *Köpke/Nemecko* (rozhl.), č. 420/07, 5. októbra 2010.

Ak ESĽP zistí, že zmluvná strana porušila niektoré z práv chránených ECHR, táto zmluvná strana je povinná vykonať rozsudok ESĽP (článok 46 ECHR). Vykonávacími opatreniami sa musí najskôr ukončiť porušovanie a musia sa v maximálnej možnej miere napraviť negatívne dôsledky porušovania s ohľadom na sťažovateľa. Vykonanie rozsudku si tiež môže vyžadovať prijatie všeobecných opatrení, ktorými sa zabráni podobnému porušovaniu, na aké poukázal ESĽP, a to prostredníctvom zmien v právnych predpisoch, prostredníctvom judikatúry alebo iných opatrení.

Ak ESĽP dospeje k záveru, že došlo k porušeniu ECHR, podľa článku 41 ECHR môže sťažovateľovi priznať „spravidlivé zadostučinenie“ na náklady zmluvnej strany.

Právo poveriť neziskový subjekt, organizáciu alebo združenie

Podľa GDPR sa umožňuje jednotlivcom, aby podali sťažnosť dozornému orgánu alebo podali žalobu na súd a aby poverili neziskový subjekt, organizáciu alebo združenie, aby ich zastupovali⁶⁴⁹. Tieto neziskové subjekty musia mať zákonné ciele vo verejnom záujme a musia pôsobiť v oblasti ochrany údajov. Môžu podať sťažnosť alebo uplatniť právo na súdny opravný prostriedok v mene dotknutej osoby (dotknutých osôb). V nariadení sa členským štátom dáva možnosť rozhodnúť – v súlade s vnútroštátnym právom – o tom, či subjekt môže podávať sťažnosti v mene dotknutých osôb bez toho, aby ich tieto osoby poverili.

Toto právo na zastupovanie umožňuje jednotlivcom využívať odborné znalosti a organizačnú a finančnú kapacitu takýchto neziskových subjektov, čím sa jednotlivcom vo veľkej miere uľahčuje uplatňovanie ich práv. Podľa GDPR sa týmto subjektom umožňuje podávať kolektívne žaloby v mene viacerých dotknutých osôb. Je to výhodné aj pre fungovanie a efektívnosť súdneho systému, keďže podobné žaloby sú zoskupené a preskúvané spoločne.

6.2.3. Zodpovednosť a právo na náhradu škody

Právo na účinný prostriedok nápravy musí jednotlivcom umožniť požadovať náhradu za škodu, ktorá im vznikla v dôsledku spracúvania ich osobných údajov, ktoré bolo v rozpore s uplatniteľnými právnymi predpismi. Zodpovednosť prevádzkovateľov a sprostredkovateľov za nezákonné spracúvanie sa výslovne uznáva v GDPR⁶⁵⁰. V tomto nariadení sa jednotlivcom priznáva právo na náhradu majetkovej

⁶⁴⁹ Všeobecné nariadenie o ochrane údajov, článok 80.

⁶⁵⁰ Tamže, článok 82.

aj nemajetkovej ujmy od prevádzkovateľa alebo sprostredkovateľa, zatiaľ čo v jeho odôvodneniach sa uvádza, že „by sa mal pojem škody vykladať v širokom zmysle spôsobom, ktorý v plnej miere zohľadňuje ciele tohto nariadenia“⁶⁵¹. Ak prevádzkovatelia nesplnia svoje povinnosti vyplývajúce z nariadenia, sú zodpovední a môžu byť predmetom žalôb o náhradu škody. Sprostredkovatelia osobných údajov sú zodpovední za škodu spôsobenú spracúvaním, len ak nesplnili povinnosti stanovené v nariadení, ktoré sa osobitne vzťahujú na sprostredkovateľov, alebo ak konali nad rámec pokynov alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom. Ak prevádzkovateľ alebo sprostredkovateľ zaplatil náhradu spôsobenej škody v plnej výške, v GDPR sa stanovuje, že má právo žiadať od ostatných prevádzkovateľov alebo sprostredkovateľov zapojených do toho istého spracúvania tú časť náhrady škody, ktorá zodpovedá ich miere zodpovednosti za škodu⁶⁵². Výnimky zo zodpovednosti sú zároveň veľmi prísne a je pri nich potrebné preukázať, že prevádzkovateľ alebo sprostredkovateľ nie je žiadnym spôsobom zodpovedný za udalosť, ktorá bola príčinou vzniknutej škody.

Náhrada škody musí byť „úplná a účinná“. Ak je škoda spôsobená spracúvaním viacerými prevádzkovateľmi a sprostredkovateľmi, každý prevádzkovateľ alebo sprostredkovateľ musí niesť zodpovednosť za celú škodu. Cieľom tohto pravidla je zabezpečiť účinnú náhradu pre dotknutú osobu a koordinovaný prístup k dodržiavaniu predpisov zo strany prevádzkovateľov a sprostredkovateľov, ktorí sa podieľajú na spracovateľských činnostiach.

Príklad: Dotknuté osoby nie sú povinné podať žalobu a žiadať náhradu škody od všetkých subjektov zodpovedných za škodu, keďže takéto konanie by mohlo byť drahé a zdĺhavé. Stačí podať žalobu proti jednému zo spoločných prevádzkovateľov, ktorý by potom mal byť zodpovedný za celú škodu. V takýchto prípadoch je prevádzkovateľ alebo sprostredkovateľ, ktorý zaplatí škodu, následne oprávnený vymáhať od ostatných subjektov, ktoré sú zapojené do spracúvania a ktoré sú zodpovedné za príslušné porušenie, sumu zaplatenú za ich časť zodpovednosti za škodu. K tomuto postupu medzi rôznymi spoločnými prevádzkovateľmi a sprostredkovateľmi dochádza po poskytnutí náhrady škody dotknutej osobe, a dotknutá osoba nie je jeho súčasťou.

651 Tamže, odôvodnenie 146.

652 Tamže, článok 82 ods. 2 a 5.

V právnom rámci RE sa v článku 12 modernizovaného Dohovoru č. 108 vyžaduje, aby zmluvné strany zaviedli vhodné prostriedky nápravy v prípade porušenia vnútroštátnych právnych predpisov, ktorými sa vykonávajú požiadavky Dohovoru. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa uvádza, že prostriedky nápravy musia zahŕňať možnosť súdneho napadnutia rozhodnutia alebo postupu a k dispozícii musia byť aj mimosúdne prostriedky nápravy⁶⁵³. Spôsoby a rôzne pravidlá týkajúce sa prístupu k týmto prostriedkom nápravy spolu s postupom, ktorý sa má dodržiavať, sú ponechané na uváženie každej zmluvnej strany. Zmluvné strany a vnútroštátne súdy by tiež mali zvážiť ustanovenia o finančnej náhrade škody v prípade materiálnej a nemateriálnej ujmy spôsobenej spracúvaním, ako aj možnosť umožnenia kolektívnych žalôb⁶⁵⁴.

6.2.4. Sankcie

Podľa **právnych predpisov RE** sa v článku 12 modernizovaného Dohovoru č. 108 uvádza, že strany musia stanoviť primerané sankcie a opravné prostriedky pre prípad porušenia ustanovení vnútroštátnych právnych predpisov, ktorými sa vykonávajú základné zásady ochrany údajov uvedené v Dohovore č. 108. V Dohovore sa nestanovuje ani neukladá osobitný súbor sankcií. Naopak, jasne sa v ňom uvádza, že každá zmluvná strana má právomoc rozhodovať o povahe súdnych alebo mimosúdnych sankcií, ktoré môžu byť trestné, správne alebo občianskoprávne. V dôvodovej správe k modernizovanému Dohovoru č. 108 sa stanovuje, že sankcie musia byť účinné, primerané a odradzujúce⁶⁵⁵. Zmluvné strany musia dodržiavať túto zásadu pri určovaní povahy a závažnosti sankcií, ktoré sú k dispozícii v ich vnútroštátnom právnom poriadku.

Podľa **právnych predpisov EÚ** sa v článku 83 GDPR splnomocňujú dozorné orgány členských štátov, aby ukladali správne pokuty za porušenia nariadenia. Výška pokút a okolností, ktoré národné orgány zohľadnia pri rozhodovaní o uložení pokuty, ako aj celkové maximálne stropy tejto pokuty sú tiež stanovené v článku 83. Režim sankcií je teda harmonizovaný v celej EÚ.

Podľa GDPR sa uplatňuje viacúrovňový prístup k pokutám. Dozorné orgány majú právomoc ukladať správne pokuty za porušenia nariadenia až do výšky 20 000 000 EUR alebo v prípade podniku 4 % jeho celkového svetového ročného

653 Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 100.

654 Tamže.

655 Tamže.

obratu – podľa toho, ktorá suma je vyššia. Porušenia, ktoré môžu viesť k tejto výške pokuty, zahŕňajú porušenia základných zásad spracúvania a podmienok súhlasu, porušenia práv dotknutých osôb a ustanovení nariadenia, ktorými sa upravuje prenos osobných údajov príjemcom v tretích krajinách. Za ostatné porušenia môžu dozorné orgány uložiť pokuty až do výšky 10 000 000 EUR alebo v prípade podniku dve percentá z celkového svetového ročného obratu – podľa toho, ktorá suma je vyššia.

Pri určovaní typu a výšky pokuty, ktoré sa majú uložiť, musia dozorné orgány zohľadniť viacero faktorov⁶⁵⁶. Musia napríklad náležite zohľadniť povahu, závažnosť a trvanie porušenia, kategórie dotknutých osobných údajov a úmyselný alebo nedbanlivostný charakter porušenia. Ak prevádzkovateľ alebo sprostredkovateľ prijal opatrenie s cieľom zmierniť škodu, ktorú utrpeli dotknuté osoby, malo by sa to zohľadniť. Podobne aj miera spolupráce s dozorným orgánom po porušení a spôsob, akým sa dozorný orgán dozvedel o porušení (napríklad, či ho informoval subjekt zodpovedný za spracúvanie alebo dotknutá osoba, ktorej práva boli porušené), sú ďalšími dôležitými faktormi, ktorými sa dozorné orgány riadia pri svojom rozhodnutí⁶⁵⁷.

Okrem právomoci ukladať správne pokuty majú dozorné orgány k dispozícii širokú škálu ďalších nápravných právomocí. Takzvané „nápravné“ právomoci dozorných orgánov sú stanovené v článku 58 GDPR. Siahajú od vydávania nariadení, upozornení a napomenutí prevádzkovateľom a sprostredkovateľom až po zavedenie dočasných, či dokonca trvalých zákazov spracovateľských činností.

Pokiaľ ide o sankcie za porušenie práva EÚ zo strany inštitúcií alebo orgánov EÚ, vzhľadom na osobitné uplatňovanie nariadenia o ochrane údajov inštitúciami EÚ sa sankcie môžu stanoviť formou disciplinárneho konania. Podľa článku 49 tohto nariadenia „za každé nedodržanie povinností podľa tohto nariadenia, či už úmyselné alebo z nedbanlivosti, podlieha úradník alebo iný zamestnanec Európskych spoločenstiev disciplinárnemu konaniu [...]“.

656 Všeobecné nariadenie o ochrane údajov, článok 83 ods. 2.

657 Pracovná skupina zriadená podľa článku 29 (2017), *Usmernenia týkajúce sa používania a stanovovania správnych pokút na účely nariadenia 2016/679*, WP 253, 3. októbra 2017.

7

Medzinárodné prenosy a toky osobných údajov

EÚ	Zahrnuté témy	RE
Prenosy osobných údajov		
Všeobecné nariadenie o ochrane údajov, článok 44	Pojem	Modernizovaný Dohovor č. 108, článok 14 ods. 1 a 2
Voľný tok osobných údajov		
Všeobecné nariadenie o ochrane údajov, článok 1 ods. 3 a odôvodnenie 170	Medzi členskými štátmi EÚ	
	Medzi zmluvnými stranami Dohovoru č. 108	Modernizovaný Dohovor č. 108, článok 14 ods. 1
Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám		
Všeobecné nariadenie o ochrane údajov, článok 45 C-362/14, <i>Maximillian Schrems/ Data Protection Commissioner</i> [VK], 2015	Rozhodnutie o primeranosti/ tretie krajiny alebo medzinárodné organizácie s primeranou úrovňou ochrany	Modernizovaný Dohovor č. 108, článok 14 ods. 2
Všeobecné nariadenie o ochrane údajov, článok 46 ods. 1 a 2	Primerané záruky vrátane vymožiteľných práv a právnych prostriedkov nápravy pre dotknuté osoby poskytované prostredníctvom štandardných zmluvných doložiek, záväzných vnútropodnikových pravidiel, kódexov správania a certifikačných mechanizmov	Modernizovaný Dohovor č. 108, článok 14 ods. 2, 3, 5 a 6

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov, článok 46 ods. 3	S výhradou povolenia príslušného dozorného orgánu: zmluvné doložky a ustanovenia uvedené v správnych dojednaniach medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi	
Všeobecné nariadenie o ochrane údajov, článok 46 ods. 5	Existujúce povolenia na základe smernice 95/46	
Všeobecné nariadenie o ochrane údajov, článok 47	Záväzné vnútropodnikové pravidlá	
Všeobecné nariadenie o ochrane údajov, článok 49	Výnimky pre osobitné situácie	Modernizovaný Dohovor č. 108, článok 14 ods. 4
Príklady: Dohoda medzi EÚ a USA o záznamoch o cestujúcich Dohoda medzi EÚ a USA o SWIFT	Medzinárodné dohody	Modernizovaný Dohovor č. 108, článok 14 ods. 3 písm. a)

Podľa právnych predpisov EÚ sa vo všeobecnom nariadení o ochrane údajov stanovuje voľný tok údajov v rámci Európskej únie. Toto nariadenie však obsahuje osobitné požiadavky týkajúce sa prenosu osobných údajov do tretích krajín mimo EÚ a medzinárodným organizáciám. V nariadení sa uznáva význam takýchto prenosov, najmä pokiaľ ide o medzinárodný obchod a spoluprácu, ale uznáva sa aj zvýšené riziko pre osobné údaje. Cieľom nariadenia je preto zabezpečiť rovnakú úroveň ochrany pre osobné údaje prenášané do tretích krajín, akú majú v rámci EÚ⁶⁵⁸. V právnych predpisoch RE sa takisto uznáva dôležitosť zavedenia pravidiel pre cezhraničné toky údajov, a to na základe voľného toku údajov medzi stranami a osobitných požiadaviek pri prenosoch do iných krajín.

7.1. Povaha prenosov osobných údajov

Hlavné body

- Právne predpisy EÚ a RE obsahujú pravidlá týkajúce sa prenosu osobných údajov príjemcom v tretích krajinách alebo medzinárodným organizáciám.
- Zabezpečenie ochrany práv dotknutej osoby pri prenose údajov mimo EÚ umožňuje, aby ochrana, ktorú poskytujú právne predpisy EÚ, nasledovala osobné údaje s pôvodom v EÚ.

⁶⁵⁸ Všeobecné nariadenie o ochrane údajov, odôvodnenie 101 a 116.

V **právnych predpisoch RE** sa opisujú cezhraničné toky údajov ako prenosy osobných údajov príjemcom, ktorí podliehajú zahraničnej judikatúre⁶⁵⁹. Cezhraničné toky údajov príjemcovi, ktorý nepodlieha judikatúre zmluvnej strany, sú povolené len vtedy, ak je zabezpečená primeraná úroveň ochrany⁶⁶⁰.

V **právnych predpisoch EÚ** sa upravuje prenos „osobných údajov, ktoré sa spracúvajú alebo sú určené na spracúvanie po prenose do tretej krajiny alebo medzinárodnej organizácii [...]“⁶⁶¹. Takéto toky údajov sú povolené len vtedy, ak sú v súlade s pravidlami stanovenými v kapitole V GDPR.

Cezhraničné toky osobných údajov sú povolené pre príjemcu, ktorý podlieha jurisdikcii zmluvnej strany alebo členského štátu podľa právnych predpisov RE alebo podľa právnych predpisov EÚ. Oba právne systémy umožňujú prenos údajov do krajiny, ktorá nie je zmluvnou stranou alebo členským štátom, za predpokladu, že sú splnené určité podmienky.

7.2. Voľný pohyb/tok osobných údajov medzi členskými štátmi alebo zmluvnými stranami

Hlavné body

- Tok osobných údajov v celej EÚ, ako aj prenosy osobných údajov medzi zmluvnými stranami modernizovaného Dohovoru č. 108 nesmú podliehať obmedzeniam. Keďže nie všetky zmluvné strany modernizovaného Dohovoru č. 108 sú členskými štátmi EÚ, prenosy z členského štátu EÚ do tretej krajiny, ktorá však je zmluvnou stranou Dohovoru č. 108, nie sú možné, pokiaľ nesplňajú podmienky stanovené v GDPR.

V **rámci právnych predpisov RE** musí existovať voľný tok osobných údajov medzi stranami modernizovaného Dohovoru č. 108. Prenos sa však môže zakázať, ak existuje „skutočné a vážne riziko, že by prenos inej strane viedol k obchádzaniu ustanovení Dohovoru“, alebo ak je zmluvná strana povinná ich obísť na základe

⁶⁵⁹ Dôvodová správa k modernizovanému Dohovoru č. 108, ods. 102.

⁶⁶⁰ Modernizovaný Dohovor č. 108, článok 14 ods. 2.

⁶⁶¹ Všeobecné nariadenie o ochrane údajov, článok 44.

„harmonizovaných pravidiel ochrany, ktoré uplatňujú štáty patriace k regionálnej medzinárodnej organizácii“⁶⁶².

Podľa právnych predpisov EÚ sú obmedzenia alebo zákazy voľného toku osobných údajov medzi členskými štátmi EÚ z dôvodov súvisiacich s ochranou fyzických osôb pri spracúvaní osobných údajov zakázané⁶⁶³. Oblasť voľného toku údajov sa rozšírila Dohodou o európskom hospodárskom priestore (EHP)⁶⁶⁴, prostredníctvom ktorej sa Island, Lichtenštajnsko a Nórsko stali súčasťou vnútorného trhu.

Príklad: Ak pobočky medzinárodnej skupiny spoločností so sídlom v niekoľkých členských štátoch EÚ, okrem iného v Slovinsku a vo Francúzsku, prenášajú osobné údaje zo Slovinska do Francúzska, slovinskými vnútroštátnymi predpismi sa tento tok údajov nesmie obmedziť ani zakázať.

Keby však daná slovinská pobočka chcela príslušné údaje preniesť do materskej spoločnosti v Malajzii, slovinský vývozca údajov musí zohľadniť pravidlá uvedené v kapitole V GDPR. Tieto ustanovenia sú určené na ochranu osobných údajov dotknutých osôb, ktoré podliehajú právomoci EÚ.

Podľa právnych predpisov EÚ sa na toky osobných údajov do členských štátov EHP na účely súvisiace s predchádzaním trestným činom, ich vyšetrovaním, odhaľovaním alebo stíhaním alebo na účel výkonu trestných sankcií vzťahuje smernica 2016/680⁶⁶⁵. Zabezpečuje sa tým aj to, aby výmena osobných údajov príslušnými orgánmi v rámci Únie nebola obmedzená alebo zakázaná z dôvodu ochrany údajov. V právnych predpisoch RE sú všetky osobné údaje (vrátane ich cezhraničného toku medzi inými stranami Dohovoru č. 108), bez výnimiek na základe účelov alebo oblastí činnosti, zahrnuté do rozsahu pôsobnosti Dohovoru č. 108, pričom zmluvné strany môžu stanoviť výnimky. Všetci členovia EHP sú takisto zmluvnými stranami Dohovoru č. 108.

662 Modernizovaný Dohovor č. 108, článok 14 ods. 1.

663 Všeobecné nariadenie o ochrane údajov, článok 1 ods. 3.

664 Rozhodnutie Rady a Komisie z 13. decembra 1993 o uzavretí Dohody o Európskom hospodárskom priestore medzi Európskymi spoločenstvami, ich členskými štátmi a Rakúskou republikou, Fínskou republikou, Islandskou republikou, Lichtenštajnským kniežatstvom, Nórskym kráľovstvom, Švédskym kráľovstvom a Švajčiarskou konfederáciou, Ú. v. ES L 1, 1994.

665 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, Ú. v. EÚ L 119, 2016.

7.3. Prenosy osobných údajov do tretích krajín/krajín, ktoré nie sú stranami Dohovoru, alebo medzinárodným organizáciám

Hlavné body

- **RE** aj **EÚ** umožňujú prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám za predpokladu, že sú splnené určité podmienky na ochranu osobných údajov.
- **V právnych predpisoch RE** možno primeranú úroveň ochrany dosiahnuť právnymi predpismi štátu alebo medzinárodnej organizácie, alebo zavedením vhodných štandardov.
- **Podľa právnych predpisov EÚ** sa prenosy môžu uskutočniť, ak tretia krajina zabezpečí primeranú úroveň ochrany alebo ak prevádzkovateľ alebo sprostredkovateľ poskytne primerané záruky vrátane vymožitelných práv dotknutých osôb a právnych prostriedkov nápravy, napríklad prostredníctvom štandardných doložiek o ochrane údajov alebo záväzných vnútropodnikových pravidiel.
- **V práve RE, ako aj práve EÚ** sa stanovujú výnimky umožňujúce prenos osobných údajov za osobitných okolností aj vtedy, keď neexistuje primeraná úroveň ochrany ani primerané záruky.

Zatiaľ čo aj podľa právnych predpisov RE, aj podľa právnych predpisov EÚ sa umožňujú toky údajov do tretích krajín alebo medzinárodným organizáciám, stanovujú sa v nich odlišné podmienky. Každý súbor podmienok zohľadňuje odlišnú štruktúru a ciele príslušnej organizácie.

Podľa **právnych predpisov EÚ** v zásade existujú dva spôsoby, ako umožniť prenos osobných údajov do tretích krajín alebo medzinárodným organizáciám. Prenosy osobných údajov sa môžu uskutočniť na základe: rozhodnutia Európskej komisie o primeranosti⁶⁶⁶; alebo, ak neexistuje takéto rozhodnutie o primeranosti, tak v prípade, ak prevádzkovateľ alebo sprostredkovateľ poskytnú dotknutej osobe primerané záruky vrátane vymožitelných práv a právnych prostriedkov nápravy⁶⁶⁷. Ak

⁶⁶⁶ Všeobecné nariadenie o ochrane údajov, článok 45.

⁶⁶⁷ Tamže, článok 46.

neexistuje rozhodnutie o primeranosti ani primerané záruky, je k dispozícii niekoľko výnimiek.

V **právnych predpisoch RE** sa však voľné prenosy údajov do krajín, ktoré nie sú stranami Dohovoru, povoľujú len na základe:

- právnych predpisov tohto štátu alebo medzinárodnej organizácie vrátane uplatniteľných medzinárodných zmlúv alebo dohôd zaručujúcich primerané záruky,
- záruk *ad hoc* alebo schválených štandardizovaných záruk, ktoré poskytujú právne záväzné a vykonateľné nástroje, ktoré prijali a vykonávajú osoby zapojené do prenosu a ďalšieho spracúvania⁶⁶⁸.

Podobne ako v právnych predpisoch EÚ je v prípade neexistencie primeranej úrovne ochrany údajov k dispozícii niekoľko výnimiek.

7.3.1. Prenosy na základe rozhodnutia o primeranosti

V **právnych predpisoch EÚ** je voľný tok osobných údajov do tretích krajín s primeranou úrovňou ochrany údajov stanovený v článku 45 GDPR. SDEÚ objasnil, že pojem „primeraná úroveň ochrany“ si vyžaduje, aby tretia krajina zabezpečila úroveň ochrany základných práv a slobôd, ktorá je „v podstate rovnocenná“⁶⁶⁹ so zárukami zaručenými právnymi predpismi v EÚ. Zároveň sa však prostriedky, ktoré tretia krajina môže využiť s cieľom zabezpečiť takúto úroveň ochrany, môžu líšiť od prostriedkov používaných v rámci EÚ, norma primeranosti si nevyžaduje napodobenie pravidiel EÚ bod za bodom⁶⁷⁰.

Európska komisia posudzuje úroveň ochrany údajov v cudzích krajinách skúmaním ich vnútroštátnych právnych predpisov a uplatniteľných medzinárodných záväzkov. Je potrebné zohľadniť aj účasť krajiny vo viacstranných alebo v regionálnych systémoch, najmä pokiaľ ide o ochranu osobných údajov. Ak Európska komisia zistí, že tretia krajina alebo medzinárodná organizácia zabezpečujú primeranú úroveň

668 Modernizovaný Dohovor č. 108, článok 14 ods. 3 písm. a) a b).

669 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015, bod 96.

670 Tamže, bod 74. Pozri aj Európska komisia (2017), oznámenie Komisie Európskemu parlamentu a Rade „Výmena a ochrana osobných údajov v globalizovanom svete“, COM (2017)7 final z 10. januára 2017, s. 6.

ochrany, môže vydať rozhodnutie o primeranosti, ktoré má záväzný účinok⁶⁷¹. SDEÚ však konštatoval, že národné dozorné orgány majú stále právomoc preskúmať žiadosť osoby v súvislosti s ochranou jej osobných údajov, ktoré boli prenesené do tretej krajiny, ktorú Komisia považuje za krajinu, ktorá zabezpečuje primeranú úroveň ochrany, ak táto osoba tvrdí, že platné právo a prax v tejto krajine nezaistujú primeranú úroveň ochrany⁶⁷².

Európska komisia môže tiež posúdiť primeranosť územia v rámci tretej krajiny alebo sa obmedziť na konkrétne odvetvia, ako to bolo napríklad v prípade kanadských právnych predpisov pre súkromnú komerčnú činnosť⁶⁷³. Existujú aj rozhodnutia o primeranosti týkajúce sa prenosov na základe dohôd medzi EÚ a tretími krajinami. Tieto rozhodnutia sa vzťahujú výlučne na jeden druh prenosu údajov, napríklad prenos záznamov o cestujúcich (PNR) od leteckého dopravcu zahraničným orgánom hraničnej kontroly v prípade, že letecký dopravca lieta z EÚ do niektorých zámorských destinácií (pozri [oddiel 7.3.4](#)).

Rozhodnutia o primeranosti sú predmetom priebežného monitorovania. Európska komisia pravidelne preskúmava takéto rozhodnutia a sleduje vývoj, ktorý by mohol ovplyvniť ich stav. Ak teda Európska komisia zistí, že tretia krajina alebo medzinárodná organizácia už nespĺňajú podmienky odôvodňujúce rozhodnutie o primeranosti, môže rozhodnutie zmeniť, pozastaviť alebo zrušiť. Komisia môže takisto začať rokovania s dotknutou treťou krajinou alebo s medzinárodnou organizáciou s cieľom vyriešiť problém súvisiaci s takýmto rozhodnutím.

Rozhodnutia o primeranosti prijaté Európskou komisiou na základe smernice 95/46/ES zostávajú v platnosti až do ich zmeny, nahradenia alebo zrušenia rozhodnutím Komisie prijatým v súlade s pravidlami uvedenými v článku 45 GDPR.

Európska komisia doteraz uznala, že primeranú ochranu poskytujú Andorra, Argentína, Faerské ostrovy, Guernsey, Izrael, Jersey, Kanada (obchodné organizácie patriace do rozsahu pôsobnosti zákona o osobných informáciách a elektronických dokumentoch – PIPEDA), Nový Zéland, Ostrov Man, Švajčiarsko a Uruguaj. Pokiaľ ide

671 Priebežne aktualizovaný zoznam krajín, na ktoré sa vzťahuje rozhodnutie o primeranosti, nájdete na domovskej stránke [Generálneho riaditeľstva Európskej komisie pre spravodlivosť](#).

672 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015, body 63 a 65 – 66.

673 Európska komisia (2002), rozhodnutie Komisie z 20. decembra 2001 podľa smernice 95/46/ES Európskeho parlamentu a Rady o primeranej ochrane osobných údajov poskytovaných kanadským Zákonom o ochrane osobných informácií a elektronických dokumentoch, Ú. v. ES L 2, 2002.

o prenosy do USA, Európska komisia prijala v roku 2000 rozhodnutie o primeranosti, ktorým sa umožňuje prenos spoločnostiam, ktoré osvedčili svoju ochranu osobných údajov prenášaných z EÚ, a súlad s tzv. „zásadami Safe Harbour“⁶⁷⁴. SDEÚ zrušil toto rozhodnutie v roku 2015 a v júli 2016 bolo prijaté nové rozhodnutie o primeranosti, ku ktorému mali spoločnosti možnosť pristúpiť od 1. augusta 2016.

Príklad: Vo veci *Schrems*⁶⁷⁵ pán Maximilian Schrems, rakúsky občan, bol používateľ Facebooku viacero rokov. Niektoré alebo všetky údaje, ktoré pán Schrems poskytol spoločnosti Facebook, boli zaslané z írskej dcérskej spoločnosti Facebook na servery nachádzajúce sa v USA, kde boli spracúvané. Pán Schrems podal sťažnosť írskemu orgánu pre ochranu osobných údajov, pričom sa domnieval, že vzhľadom na odhalenia amerického oznamovateľa Edwarda Snowdena týkajúce sa sledovacích činností informačných služieb Spojených štátov právne predpisy a postupy Spojených štátov neposkytujú dostatočnú ochranu údajov prenášaných do tejto krajiny. Írsky orgán sťažnosť zamietol z dôvodu, že Komisia vo svojom rozhodnutí z 26. júla 2000 usúdila, že v rámci systému „Safe Harbour“ Spojené štáty zabezpečujú primeranú úroveň ochrany prenášaných osobných údajov. Vec bola podaná na írsky High Court (Vyšší súd), ktorý ju postúpil SDEÚ na prejudiciálne konanie.

SDEÚ rozhodol, že rozhodnutie Komisie o primeranosti rámca Safe Harbour bolo neplatné. SDEÚ najprv konštatoval, že rozhodnutím sa umožnilo obmedzenie dodržiavanie zásad rámca Safe Harbour na ochranu údajov na základe požiadaviek národnej bezpečnosti, verejného záujmu alebo presadzovania práva alebo na základe vnútroštátnych právnych predpisov USA. Toto rozhodnutie teda umožnilo zásah do základných práv tých osôb, ktorých osobné údaje boli alebo mohli byť prenášané do USA⁶⁷⁶. Ďalej uviedol, že rozhodnutie neobsahuje žiadne ustanovenie týkajúce sa existencie pravidiel v Spojených štátoch, ktoré by boli určené na obmedzenie takýchto zásahov, ani existencie akejkoľvek účinnej právnej ochrany proti takýmto zásahom⁶⁷⁷. SDEÚ zdôraznil, že pokiaľ ide o úroveň ochrany základných práv a slobôd

674 Rozhodnutie Komisie 2000/520/ES z 26. júla 2000 v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej zásadami „bezpečného prístavu“ a súvisiacimi často kladenými otázkami vydanými Ministerstvom obchodu USA, Ú. v. ES L 215. Rozhodnutie bolo vyhlásené za neplatné Súdnym dvorom Európskej únie vo veci C-632/14, *Maximilian Schrems/Data Protection Commissioner* [VK].

675 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

676 Tamže, bod 84.

677 Tamže, body 88 – 89.

zaručenú v rámci Únie, jej právna úprava obsahujúca zásah do článkov 7 a 8 Charty musí stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie opatrenia a stanovujúce minimálne záruky, výnimky a obmedzenia týkajúce sa ochrany osobných údajov⁶⁷⁸. Vzhľadom na to, že v rozhodnutí Komisie sa neuvádza, že Spojené štáty v skutočnosti zaistujú takúto úroveň ochrany z dôvodu svojho vnútroštátneho práva alebo medzinárodných záväzkov, SDEÚ dospel k záveru, že nespĺňa požiadavky príslušného ustanovenia o prenose údajov v smernici o ochrane údajov, a preto je neplatné⁶⁷⁹.

Úroveň ochrany Spojených štátov teda nebola „v podstate rovnocenná“ so základnými právami a slobodami zaručenými v EÚ⁶⁸⁰. SDEÚ uviedol, že boli porušené rôzne články Charty základných práv Európskej únie. Po prvé bola ohrozená podstata článku 7, pretože právne predpisy Spojených štátov „[umožňovali] orgánom verejnej moci všeobecný prístup k obsahu elektronických komunikácií“. Po druhé bola porušená aj podstata článku 47, pretože právne predpisy neposkytovali jednotlivcom právne prostriedky nápravy, pokiaľ ide o prístup k osobným údajom alebo opravu či vymazanie osobných údajov. Napokon, vzhľadom na to, že dohodou o Safe Harbour boli porušené uvedené články, osobné údaje už neboli spracúvané zákonným spôsobom, čo viedlo k porušeniu článku 8.

Po tom, ako SDEÚ vyhlásil dohodu o Safe Harbour za neplatnú, Komisia a USA sa dohodli na novom rámci – Privacy Shield medzi EÚ a USA. Komisia prijala 12. júla 2016 rozhodnutie, v ktorom vyhlasuje, že Spojené štáty zabezpečujú primeranú úroveň ochrany osobných údajov prenášaných z Únie do organizácií v Spojených štátoch v rámci Privacy Shield⁶⁸¹.

678 Tamže, body 91 – 92.

679 Tamže, body 96 – 97.

680 Tamže, body 73 – 74 a 96.

681 *Vykonávacie rozhodnutie Komisie (EÚ) 2016/1250 z 12. júla 2016 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA, Ú. v. EÚ L 207*. Pracovná skupina zriadená podľa článku 29 uvítala zlepšenia, ktoré priniesol mechanizmus Privacy Shield v porovnaní s rozhodnutím o Safe Harbour, a ocenila, že Komisia a orgány Spojených štátov zohľadnili v konečnej verzii dokumentov týkajúcich sa Privacy Shield obavy vyjadrené v jej stanovisku WP 238 k návrhu rozhodnutia o primeranosti Privacy Shield medzi EÚ a USA. Poukázala však na viaceré nevyriešené otázky. Pozri aj: pracovná skupina zriadená podľa článku 29, *Stanovisko 01/2016 k návrhu rozhodnutia o primeranosti štítu na ochranu osobných údajov medzi EÚ a USA*, prijaté 13. apríla 2016, 16/SK WP 238.

Podobne ako v prípade dohody o Safe Harbour sa rámec Privacy Shield medzi EÚ a USA zameriava na ochranu osobných údajov, ktoré sa prenášajú z EÚ do USA na obchodné účely⁶⁸². Spoločnosti zo Spojených štátov môžu dobrovoľne osvedčiť, že sa zaviazali dodržiavať normy ochrany údajov v rámci zoznamu organizácií zapojených do Privacy Shield. Príslušné orgány Spojených štátov monitorujú a overujú, že spoločnosti, ktoré osvedčili dodržiavanie týchto noriem, ich aj dodržiajú.

V rámci systému Privacy Shield sú stanovené najmä:

- povinnosti v oblasti ochrany údajov týkajúce sa spoločností, ktoré prijímajú osobné údaje z EÚ,
- ochrana jednotlivcov a možnosť nápravy, najmä zriadenie mechanizmu ombudsmana, ktorý je nezávislý od spravodajských služieb Spojených štátov a zaoberá sa sťažnosťami jednotlivcov, ktorí sa domnievajú, že orgány Spojených štátov nezákonným spôsobom použili ich osobné údaje v oblasti národnej bezpečnosti,
- každoročné spoločné preskúmanie na monitorovanie vykonávania tohto rámca⁶⁸³, prvé preskúmanie sa uskutočnilo v septembri 2017⁶⁸⁴.

Vláda Spojených štátov poskytla písomné záväzky a záruky, ktoré sú pripojené k rozhodnutiu o Privacy Shield. Obsahujú obmedzenia a záruky týkajúce sa prístupu vlády Spojených štátov k osobným údajom na účely presadzovania práva a národnej bezpečnosti.

7.3.2. Prenosy vyžadujúce si primerané záruky

V **právnych predpisoch EÚ a RE** sa uznávajú primerané záruky medzi prevádzkovateľom prenášajúcim údaje a príjemcom v tretej krajine alebo medzinárodnej organizácii ako možný prostriedok na zabezpečenie dostatočnej úrovne ochrany údajov pre príjemcu.

Podľa **právnych predpisov EÚ** sú prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii povolené, ak prevádzkovateľ alebo sprostredkovateľ

682 Ďalšie informácie nájdete v informačnom prehľade EU-U.S. Privacy Shield factsheet.

683 Viac informácií nájdete na webovej stránke Európskej komisie o Privacy Shield medzi EÚ a USA.

684 Európska komisia, *Správa Komisie Európskemu parlamentu a Rade o prvom každoročnom preskúmaní fungovania štítu na ochranu osobných údajov medzi EÚ a USA*, COM (2017)611 final, 18. októbra 2017. Pozri tiež pracovná skupina zriadená podľa článku 29, *Štít na ochranu osobných údajov medzi EÚ a USA – prvé každoročné preskúmanie*, prijaté 28. novembra 2017, 17/EN WP 255.

poskytujú primerané záruky a vymožitelné práva a ak dotknuté osoby majú k dispozícii účinné právne prostriedky nápravy⁶⁸⁵. Zoznam prijateľných „primeraných záruk“ sa uvádza výlučne v právnych predpisoch EÚ o ochrane údajov. Primerané záruky sa môžu stanoviť pomocou:

- právne záväzného a vykonateľného nástroja medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi,
- záväzných vnútropodnikových pravidiel,
- štandardných doložiek o ochrane údajov, ktoré prijala buď Európska komisia, alebo dozorný orgán,
- kódexov správania,
- certifikačných mechanizmov⁶⁸⁶.

Prispôbené zmluvné doložky medzi prevádzkovateľom alebo sprostredkovateľom v EÚ a príjemcom údajov v tretej krajine sú ďalším prostriedkom na poskytnutie primeraných záruk. Takéto zmluvné doložky však musí schváliť príslušný dozorný orgán predtým, ako je možné ich využiť ako nástroj na prenos osobných údajov. Podobne môžu orgány verejnej moci využiť ustanovenia o ochrane údajov, ktoré sa vložila do správnych dojednaní za predpokladu, že to dozorný orgán povolil⁶⁸⁷.

V právnych predpisoch RE sú povolené toky údajov do štátu alebo medzinárodnej organizácii, ktorá nie je stranou modernizovaného Dohovoru č. 108, za predpokladu, že je zabezpečená primeraná úroveň ochrany. Možno ju zabezpečiť:

- právnymi predpismi štátu alebo medzinárodnej organizácie alebo
- zárukami ad hoc alebo štandardizovanými zárukami zakotvenými v právne záväznom dokumente⁶⁸⁸.

685 Všeobecné nariadenie o ochrane údajov, článok 46.

686 Všeobecné nariadenie o ochrane údajov, článok 46 ods. 1 písm. c) a d), článok 46 ods. 2 písm. a), b), e) a f) a článok 47.

687 Tamže, článok 46 ods. 3.

688 Modernizovaný Dohovor č. 108, článok 14 ods. 3 písm. b).

Prenosy, na ktoré sa vzťahujú zmluvné doložky

V **právnych predpisoch RE**, ako aj **EÚ** sú uvedené zmluvné doložky medzi prevádzkovateľom exportujúcim údaje a príjemcom v tretej krajine ako možné prostriedky na zaručenie dostatočnej úrovne ochrany údajov u príjemcu⁶⁸⁹.

Na úrovni EU vypracovala Európska komisia za pomoci pracovnej skupiny zriadenej podľa článku 29 štandardné zmluvné doložky, ktoré boli úradne osvedčené rozhodnutím Komisie ako doklad o primeranej ochrane údajov⁶⁹⁰. Keďže rozhodnutia Komisie sú v členských štátoch záväzné v celom rozsahu, vnútroštátne orgány poverené dozorom nad cezhraničnými tokmi údajov musia vo svojich postupoch uznávať tieto zmluvné doložky⁶⁹¹. Ak sa teda prevádzkovateľ exportujúci údaje a príjemca v tretej krajine dohodnú a podpíšu uvedené opatrenia, mali by dozornému orgánu poskytnúť dostatočný dôkaz o uplatnení primeraných záruk. Vo veci *Schrems* však SDEÚ rozhodol, že Európska komisia nemá právomoc obmedziť právomoci národných dozorných orgánov pri dohľade nad prenosom osobných údajov do tretej krajiny, ktorá bola predmetom rozhodnutia Komisie o primeranosti⁶⁹². Národným dozorným orgánom sa preto nebráni vykonávať svoje právomoci vrátane právomoci pozastaviť alebo zakázať prenos osobných údajov v prípade, že sa prenos vykonáva v rozpore s právnymi predpismi EÚ alebo vnútroštátnymi právnymi predpismi o ochrane údajov, napríklad keď poskytovateľ údajov nedodržiava štandardné zmluvné doložky⁶⁹³.

Existencia štandardných zmluvných opatrení v právnom rámci EÚ nebráni prevádzkovateľom, aby sformulovali iné zmluvné doložky *ad hoc*, pokiaľ dozorný orgán tieto doložky schválil⁶⁹⁴. Mali by však zaisťovať rovnakú úroveň ochrany, akú poskytujú štandardné zmluvné doložky. Pri schvaľovaní doložiek *ad hoc* sa od dozorných orgánov vyžaduje, aby uplatňovali mechanizmus konzistentnosti na zabezpečenie

689 Všeobecné nariadenie o ochrane údajov, článok 46 ods. 3; modernizovaný Dohovor č. 108, článok 14 ods. 3 písm. b).

690 Tamže, článok 46 ods. 2 písm. b) a článok 46 ods. 5.

691 Tamže, článok 46 ods. 2 písm. c); Zmluva o fungovaní Európskej únie, článok 288.

692 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. október 2015, body 96 – 98 a 102 – 105.

693 Komisia zmenila svoje rozhodnutie o štandardných zmluvných doložkách tak, aby zohľadnila stanovisko SDEÚ vo veci *Schrems*. *Vykonávacie rozhodnutie Komisie (EÚ) 2016/2297* zo 16. decembra 2016, ktorým sa menia rozhodnutia 2001/497/ES a 2010/87/EÚ o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín a spracovateľom usadeným v takýchto krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES, Ú. v. EÚ L 344, 2016.

694 Všeobecné nariadenie o ochrane údajov, článok 46 ods. 3 písm. a)

jednotného regulačného prístupu v rámci celej EÚ⁶⁹⁵. To znamená, že príslušný dozorný orgán musí svoj návrh rozhodnutia o doložkách predložiť EDPB. EDPB vydá stanovisko k tejto záležitosti a dozorný orgán musí toto stanovisko v čo najväčšej miere zohľadniť pri vypracúvaní rozhodnutia. Ak dozorný orgán nemá v úmysle riadiť sa stanoviskom EDPB, uplatní sa mechanizmus riešenia sporov v rámci EDPB a Výbor prijme záväzné rozhodnutie⁶⁹⁶.

Medzi najdôležitejšie vlastnosti štandardných zmluvných opatrení patrí:

- opatrenie týkajúce sa oprávnenej osoby tretej strany, ktoré umožňuje dotknutým osobám, aby vykonávali zmluvné práva dokonca aj vtedy, keď nie sú zmluvnou stranou,
- súhlas príjemcu údajov alebo dovozcu s tým, že sa v prípade sporu podrobí postupu vnútroštátneho dozorného orgánu a/alebo súdu v krajine prevádzkovateľa exportujúceho údaje.

V súčasnosti sú k dispozícii dva súbory štandardných doložiek pre prenosy medzi prevádzkovateľmi, z ktorých si prevádzkovateľ exportujúci údaje môže vybrať⁶⁹⁷. V prípade prenosov od prevádzkovateľa k sprostredkovateľovi existuje len jeden súbor štandardných zmluvných doložiek⁶⁹⁸. Tieto štandardné zmluvné doložky sú však v súčasnosti predmetom súdneho konania.

Príklad: Po tom, ako SDEÚ vyhlásil rozhodnutie o Safe Harbour za neplatné⁶⁹⁹, prenosy osobných údajov do USA sa už nemohli zakladať na tomto rozhodnutí o primeranosti. Zatiaľ čo prebiehali rokovania s americkými orgánmi

695 Tamže, článok 63 a článok 64 ods. 1 písm. e).

696 Tamže, články 64 a 65.

697 Súbor I je súčasťou prílohy k dokumentu Európskej komisie (2001), rozhodnutie Komisie 2001/497/ES z 15. júna 2001 o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín podľa smernice 95/46/ES, Ú. v. ES L 181, 2001; súbor II je súčasťou prílohy k dokumentu Európskej komisie (2004), rozhodnutie Komisie 2004/915/ES z 27. decembra 2004, ktorým sa mení a dopĺňa rozhodnutie 2001/497/ES o zavedení alternatívneho súboru o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín, Ú. v. EÚ L 385, 2004.

698 Európska komisia (2010), rozhodnutie Komisie 2010/87 z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES, Ú. v. EÚ L 39, 2010. V čase vypracovania príručky bolo používanie štandardných zmluvných doložiek ako základu pre prenosy osobných údajov do Spojených štátov predmetom súdneho konania pred írskym High Court.

699 SDEÚ, C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015.

a očakávalo sa prijatie nového rozhodnutia o primeranosti (napokon prijaté 12. júla 2016), prenosy sa mohli uskutočniť len na základe iných právnych základov, ako sú štandardné zmluvné doložky alebo záväzné vnútropodnikové pravidlá⁷⁰⁰. Viaceré spoločnosti vrátane spoločnosti Facebook Ireland (proti ktorým bola podaná žaloba, ktorá viedla k zrušeniu rozhodnutia o Safe Harbour) prešli na štandardné zmluvné doložky, aby mohli pokračovať vo svojich prenosoch údajov medzi EÚ a USA.

Pán Schrems podal sťažnosť na írsky dozorný orgán a požiadal ho o pozastavenie prenosu údajov do USA na základe štandardných zmluvných doložiek. V podstate tvrdil, že keď sa jeho osobné údaje prenášajú z írskej dcérskej spoločnosti Facebook do spoločnosti Facebook Inc. a na servery umiestnené v USA, neexistuje záruka, že budú chránené. Spoločnosť Facebook Inc. je viazaná americkými zákonmi, ktoré by jej mohli ukladať povinnosť zverejňovať osobné údaje americkým orgánom presadzovania práva, a nie je k dispozícii žiadny súdny prostriedok nápravy pre európskych jednotlivcov, aby takýto postup mohli napadnúť⁷⁰¹. Z týchto dôvodov SDEÚ dospel k záveru, že rozhodnutie o Safe Harbour je neplatné, a hoci sa rozsudok súdu obmedzil na preskúmanie tohto rozhodnutia, žalobca sa domnieval, že tieto otázky sú relevantné aj v prípadoch, keď k prenosu dochádza na základe zmluvných doložiek. V čase vypracúvania tejto príručky sa prípad skúmal na írskom najvyššom súde. Žalobca má podľa všetkého v úmysle obrátiť sa na SDEÚ a napadnúť platnosť rozhodnutia Európskej komisie o štandardných zmluvných doložkách. Ako sa uvádza v kapitole 5, len SDEÚ má právomoc vyhlásiť nástroj EÚ za neplatný.

Prenosy, na ktoré sa vzťahujú záväzné vnútropodnikové pravidlá

Právne predpisy EÚ umožňujú prenosy osobných údajov aj na základe záväzných vnútropodnikových pravidiel pre medzinárodné prenosy, ktoré sa uskutočňujú v rámci tej istej skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti⁷⁰². Predtým, ako sa záväzné vnútropodnikové pravidlá možno spo-

700 Vykonávacie rozhodnutie Komisie (EÚ) 2016/1250 z 12. júla 2016 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA, Ú. v. EÚ L 207.

701 Ďalšie informácie nájdete v [revidovanej sťažnosti](#) proti spoločnosti Facebook Ireland Ltd, ktorú írskemu komisárovi pre ochranu údajov predložil pán Maximilian Schrems 1. decembra 2015.

702 Všeobecné nariadenie o ochrane údajov, článok 47.

ľahnúť ako na nástroj na prenos osobných údajov, príslušný dozorný orgán ich musí schváliť v súlade so záväznými vnútropodnikovými pravidlami, za použitia mechanizmu konzistentnosti.

Schválenie záväzných vnútropodnikových pravidiel si vyžaduje, aby boli pravidlá právne záväzné, aby zahŕňali všetky základné zásady ochrany údajov a aby sa vzťahovali na každého člena skupiny a každý člen ich uplatňoval. Musia výslovne udeliť vymáhateľné práva dotknutým osobám, zahŕňať všetky základné zásady ochrany údajov a spĺňať určité formálne požiadavky, napríklad uvádzať štruktúru podniku, opísať prenosy a spôsob, akým sa zásady ochrany údajov budú uplatňovať. Zahŕňa to poskytovanie takýchto informácií dotknutým osobám. V záväzných vnútropodnikových pravidlách sa musia okrem iného špecifikovať práva dotknutých osôb a ustanovenia o zodpovednosti za akékoľvek porušenie týchto pravidiel⁷⁰³. Pri schvaľovaní záväzných vnútropodnikových pravidiel sa uplatňuje mechanizmus konzistentnosti pre spoluprácu orgánov dohľadu (opísaný v kapitole 5).

Vedúci dozorný orgán v rámci mechanizmu konzistentnosti preskúma navrhované záväzné vnútropodnikové pravidlá, prijme návrh rozhodnutia a oznamuje ho EDPB. Výbor vydá stanovisko k tejto záležitosti a vedúci dozorný orgán môže formálne schváliť záväzné vnútropodnikové pravidlá, pričom „v čo najväčšej miere“ zohľadní stanovisko Výboru. Toto stanovisko nie je právne záväzné, ale ak má dozorný orgán v úmysle podľa tohto stanoviska nepostupovať, aktivuje sa mechanizmus riešenia sporov a Výbor bude musieť prijať právne záväzné rozhodnutie dvoj tretinovou väčšinou svojich členov⁷⁰⁴.

V **právnych predpisoch RE** k *ad hoc* zárukám alebo štandardizovaným zárukám, ktoré sú súčasťou právne záväzného dokumentu⁷⁰⁵, patria aj záväzné vnútropodnikové pravidlá.

7.3.3. Výnimky pre osobitné situácie

Podľa právnych predpisov EÚ môže byť prenos osobných údajov do tretej krajiny odôvodnený aj vtedy, ak neexistuje rozhodnutie o primeranosti alebo záruky,

703 Podrobnejší opis sa nachádza v článku 47 všeobecného nariadenia o ochrane údajov.

704 Tamže, článok 57 ods. 1 písm. s), článok 58 ods. 1 písm. j), článok 64 ods. 1 písm. f), článok 65 ods. 1 a 2.

705 Modernizovaný Dohovor č. 108, článok 14 ods. 3 písm. b).

napríklad štandardné zmluvné doložky alebo záväzné vnútropodnikové pravidlá, a to v prípade jednej z týchto okolností:

- dotknutá osoba výslovne súhlasí s prenosom údajov,
- dotknutá osoba uzatvára – alebo sa pripravuje na uzatvorenie – zmluvného vzťahu, v rámci ktorého je prenos údajov do zahraničia nevyhnutný,
- na uzatvorenie zmluvy medzi prevádzkovateľom a tretou stranou v záujme dotknutej osoby,
- z dôležitých dôvodov verejného záujmu,
- na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov,
- na ochranu životne dôležitých záujmov dotknutej osoby,
- na prenos údajov z verejných registrov (ide o prípad prevládajúceho záujmu širokej verejnosti o prístup k informáciám uloženým vo verejných registroch)⁷⁰⁶.

Ak sa neuplatňuje žiadna z týchto podmienok a ak sa prenosi nemôžu zakladať na rozhodnutí o primeranosti alebo primeraných zárukách, prenos sa môže uskutočniť len vtedy, ak nie je opakujúcej sa povahy, týka sa len obmedzeného počtu dotknutých osôb, je nevyhnutný na účely závažných oprávnených záujmov, ktoré sleduje prevádzkovateľ a nad ktorými neprevažujú záujmy alebo práva a slobody dotknutej osoby⁷⁰⁷. V týchto prípadoch musí prevádzkovateľ posúdiť okolnosti sprevádzajúce prenos údajov a poskytnúť záruky. Musí tiež informovať dozorný orgán a príslušné dotknuté osoby o prenose, ako aj o oprávnených záujmoch, ktoré ho odôvodňujú.

To, že výnimky sú poslednou možnosťou pre zákonné prenosi⁷⁰⁸ (majú sa použiť len v prípade, že neexistuje rozhodnutie o primeranosti ani žiadne iné záruky), zdôrazňuje ich výnimočný charakter a táto skutočnosť je ďalej zdôraznená v odôvodneniach GDPR⁷⁰⁹. Výnimky ako také sa akceptujú ako možnosť pre „prenosi za určitých okolností“ na základe súhlasu, a ak „prenos je občasný a potrebný“⁷¹⁰ v súvislosti so zmluvou alebo právnym nárokom.

⁷⁰⁶ Všeobecné nariadenie o ochrane údajov, článok 49.

⁷⁰⁷ Tamže.

⁷⁰⁸ Tamže, článok 49 ods. 1.

⁷⁰⁹ Pozri všeobecné nariadenie o ochrane údajov, článok 49 ods. 1 písm. a), b) a e) a odôvodnenie 113.

⁷¹⁰ Tamže, článok 49 ods. 1.

Okrem toho, podľa usmernení pracovnej skupiny zriadenej podľa článku 29 musia byť výnimky pre osobitné situácie výnimočné, a to na základe posúdenia jednotlivých prípadov, a nemôžu sa použiť na hromadné alebo opakované prenosy⁷¹¹. Európsky dozorný úradník pre ochranu údajov takisto zdôraznil mimoriadny charakter výnimiek používaných ako právny základ pre prenosy podľa nariadenia č. 45/2001, pričom poznamenal, že toto riešenie by sa malo používať „v obmedzených prípadoch“ a „pri príležitostných prenosoch“⁷¹².

Príklad: Spoločnosť prevádzkujúca globálny distribučný systém (GDS) so sídlom v Spojených štátoch poskytuje online rezervačný systém pre viaceré letecké spoločnosti, hotely a výletné plavby po celom svete a spracúva údaje desiatok miliónov osôb v EÚ. Pri prvotnom prenose údajov na svoje servery v Spojených štátoch sa táto spoločnosť spolieha na výnimku ako na zákonný základ pre tieto prenosy, a to na potrebu uzatvoriť zmluvu. Neposkytuje teda žiadne iné záruky týkajúce sa osobných údajov pochádzajúcich z Európy, ktoré boli prenesené do Spojených štátov a následne poskytnuté hotelom po celom svete (to znamená žiadne záruky pri ďalších prenosoch). Táto spoločnosť nespĺňa požiadavky GDPR na zákonné medzinárodné prenosy údajov, pretože sa odvoláva na výnimku ako na právny základ pre hromadné prenosy.

Pokiaľ nie je prijaté rozhodnutie o primeranosti, EÚ alebo jej členské štáty sú oprávnené stanoviť obmedzenia pre prenos osobitných kategórií osobných údajov do tretej krajiny napriek tomu, že sú splnené ďalšie podmienky pre takéto prenosy, a to zo závažných dôvodov verejného záujmu. Tieto obmedzenia by sa mali vnímať ako výnimočné a členské štáty sú povinné oznámiť príslušné ustanovenia Komisii⁷¹³.

Podľa **právnych predpisov RE** sa umožňuje tok údajov na územia, ktoré nemajú primeranú ochranu údajov v prípadoch, keď:

- dotknutá osoba poskytla súhlas,
- záujmy dotknutej osoby si takýto prenos vyžadujú,

711 Pracovná skupina zriadená podľa článku 29 (2005), *Pracovný dokument o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995*, WP 114, Brusel, 25. novembra 2005.

712 Európsky dozorný úradník pre ochranu údajov, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, pozičný dokument, Brusel, 14. júla 2014, s. 15.

713 Pozri všeobecné nariadenie o ochrane údajov, článok 49 ods. 5.

- existujú prevažujúce oprávnené záujmy, najmä dôležité verejné záujmy stanovené zákonom,
- ide o nevyhnutné a primerané opatrenie v demokratickej spoločnosti⁷¹⁴.

7.3.4. Prenosy na základe medzinárodných dohôd

EÚ môže uzatvárať medzinárodné dohody s tretími krajinami, ktorými sa upravuje prenos osobných údajov na konkrétne účely. Tieto dohody musia obsahovať primerané záruky na zabezpečenie ochrany osobných údajov dotknutých osôb. GDPR týmito medzinárodnými dohodami nie je dotknutá⁷¹⁵.

Členské štáty môžu takisto uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktoré poskytujú primeranú úroveň ochrany základných práv a slobôd fyzických osôb, pokiaľ tieto dohody nemajú vplyv na uplatňovanie GDPR.

Podobné pravidlo je uvedené v článku 12 ods. 3 písm. a) modernizovaného Dohovoru č. 108.

Príkladmi medzinárodných dohôd týkajúcich sa prenosu osobných údajov sú dohody o záznamoch o cestujúcich (PNR).

Záznamy o cestujúcich

Údaje zo záznamov o cestujúcich (PNR) zbierajú letecké spoločnosti v rámci rezervácie letenky, pričom ide o meno, adresu, údaje o platobnej karte a číslo sedadla cestujúceho. Letecké spoločnosti získavajú tieto informácie aj na svoje vlastné obchodné účely. EÚ uzavrela s určitými tretími krajinami (Austráliou, Kanadou a USA) dohody o prenose údajov PNR na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov alebo závažnej nadnárodnej trestnej činnosti. Okrem toho prijala Únia v roku 2016 smernicu (EÚ) 2016/681, známu ako smernica EÚ o PNR⁷¹⁶. V tejto smernici sa stanovuje právny rámec pre členské štáty EÚ na prenos údajov PNR príslušným orgánom v iných tretích krajinách na účely prevencie, odhaľovania,

⁷¹⁴ Modernizovaný Dohovor č. 108, článok 14 ods. 4.

⁷¹⁵ Všeobecné nariadenie o ochrane údajov, odôvodnenie 102.

⁷¹⁶ [Smernica Európskeho parlamentu a Rady \(EÚ\) 2016/681](#) z 27. apríla 2016 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti, Ú. v. EÚ L 119, 2016.

vyšetrovania a stíhania teroristických trestných činov alebo závažnej trestnej činnosti. K prenosom PNR orgánom tretích krajín dochádza na individuálnom základe a sú predmetom individuálneho posúdenia toho, či je prenos potrebný na účely uvedené v smernici a za predpokladu, že sú dodržané základné práva.

Pokiaľ ide o dohody o PNR medzi EÚ a tretími krajinami, ich zlučiteľnosť so základnými právami na súkromie a ochranu údajov zakotvenými v Charte základných práv EÚ bola spochybnená. Keď po rokovaníach s Kanadou EÚ v roku 2014 podpísala dohodu o prenose a spracúvaní údajov PNR, Európsky parlament sa rozhodol postúpiť vec SDEÚ na posúdenie zákonnosti dohody z hľadiska práva EÚ, a najmä článkov 7 a 8 Charty.

Príklad: Vo svojom stanovisku k zákonnosti dohody o PNR medzi EÚ a Kanadou⁷¹⁷ SDEÚ konštatoval, že zamýšľaná dohoda je v súčasnej podobe nezlučiteľná so základnými právami uznanými v Charte, a preto nemohla byť uzavretá. Keďže išlo o spracúvanie osobných údajov, predstavovala zásah do práva na ochranu osobných údajov chráneného podľa článku 8 Charty. Zároveň išlo o obmedzenie práva na rešpektovanie súkromného života zakotveného v článku 7, vzhľadom na to, že údaje PNR sa ako celok môžu zhromažďovať a analyzovať spôsobom, ktorý odhaľuje cestovné zvyky, vzťahy medzi rôznymi osobami, informácie o ich finančnej situácii, stravovacie návyky a zdravotný stav, čo ovplyvňuje ich súkromný život.

Zásahom do základných práv, ktorý zamýšľaná dohoda predstavuje, sa sleduje cieľ všeobecného záujmu, a to cieľ verejnej bezpečnosti a boja proti terorizmu a závažnej nadnárodnej trestnej činnosti. SDEÚ však pripomenul, že na to, aby bol zásah odôvodnený, musí sa obmedziť na to, čo je nevyhnutne potrebné na dosiahnutie sledovaného cieľa. SDEÚ po analýze ustanovení dohody dospel k záveru, že zamýšľaná dohoda nespĺňa kritérium „striktnej nevyhnutnosti“. Medzi faktory, na základe ktorých SDEÚ dospel k tomuto záveru, patrili:

- Skutočnosť, že na základe zamýšľanej dohody sa mali prenášať citlivé údaje. Údaje z PNR získavané podľa zamýšľanej dohody môžu zahŕňať citlivé údaje, ako sú informácie odhaľujúce rasový alebo etnický pôvod, náboženské presvedčenie alebo zdravotný stav cestujúceho.

717 SDEÚ, *Stanovisko 1/15 Súdného dvora (veľká komora)*, 26. júla 2017.

Prenos a spracúvanie citlivých údajov zo strany kanadských orgánov by mohli ohrozovať zásadu nediskriminácie, a preto si vyžadovali presné a dôkladné odôvodnenie na základe iných dôvodov, než je verejná bezpečnosť a boj proti závažnej trestnej činnosti. V zamýšľanej dohode sa takéto odôvodnenie neposkytlo⁷¹⁸.

- Uchovávanie údajov PNR všetkých cestujúcich počas obdobia piatich rokov aj po ich odchode z Kanady sa tiež považovalo nad rámec toho, čo je striktné nevyhnutné. SDEÚ dospel k záveru, že by bolo prípustné, aby kanadské orgány uchovávali údaje o cestujúcich, pri ktorých objektívne skutočnosti naznačujú, že môžu predstavovať hrozbu pre verejnú bezpečnosť, a to aj po odchode týchto osôb z Kanady. Naopak, uchovávanie osobných údajov *všetkých* cestujúcich, pri ktorých neexistuje ani nepriamy dôkaz, že by predstavovali riziko pre verejnú bezpečnosť, nie je odôvodnené⁷¹⁹.

Poradný výbor pre Dohovor č. 108 poskytol stanovisko k vplyvu dohôd o PNR na ochranu údajov v rámci právnych predpisov Rady Európy⁷²⁰.

Údaje v správach

Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT) so sídlom v Belgicku, ktorá je sprostredkovateľom väčšiny celosvetových prevodov peňazí z európskych bánk, prevádzkovala „zrkadlové“ stredisko v Spojených štátoch amerických a musela reagovať na žiadosť ministerstva financií USA o zverejnenie údajov na účely vyšetrovania terorizmu v rámci jeho Programu na sledovanie financovania terorizmu⁷²¹.

718 Tamže, bod 165.

719 Tamže, body 204 – 207.

720 Rada Európy, *Stanovisko k dôsledkom spracúvania záznamov o cestujúcich v oblasti ochrany osobných údajov*, T-PD(2016)18rev, 19. augusta 2016.

721 Pozri v tejto súvislosti dokument pracovnej skupiny zriadenej podľa článku 29 (2011), *Stanovisko č. 14/2011 k otázkam ochrany údajov súvisiacich s predchádzaním praniu špinavých peňazí a financovaniu terorizmu*, WP 186, Brusel, 13. júna 2011; Pracovná skupina zriadená podľa článku 29 (2006), *Stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT)*, WP 128, Brusel, 22. november 2006; belgická komisia pre ochranu súkromia (*Commission de la protection de la vie privée*) (2008), „Control and recommendation procedure initiated with respect to the company SWIFT srl“, rozhodnutie, 9. decembra 2008.

Z hľadiska EÚ neexistoval žiadny dostatočný právny dôvod na poskytnutie týchto údajov – prevažne o občanoch v EÚ – do USA len preto, lebo tam sídlilo jedno zo servisných stredísk na spracúvanie údajov spoločnosti SWIFT.

V roku 2010 bola uzatvorená zvláštna dohoda medzi EÚ a USA, známa ako dohoda o spoločnosti SWIFT, s cieľom poskytnúť nevyhnutný právny základ a zaistiť primeranú úroveň ochrany údajov⁷²².

Podľa tejto dohody sa finančné údaje uchovávané spoločnosťou SWIFT naďalej poskytujú ministerstvu financií USA na účely prevencie, vyšetrovania, zisťovania a stíhania terorizmu alebo financovania terorizmu. Ministerstvo financií USA môže požadovať poskytnutie finančných údajov od spoločnosti SWIFT pod podmienkou, že žiadosť:

- čo najjasnejšie vymedzuje finančné údaje,
- jasne zdôvodňuje nevyhnutnosť údajov,
- je vypracovaná čo najužšie s cieľom minimalizovať objem požadovaných údajov,
- nepožaduje poskytnutie žiadnych údajov týkajúcich sa jednotnej oblasti platieb v eurách (SEPA)⁷²³.

Kópia každej žiadosti ministerstva financií USA sa musí zaslať Europolu a Europol musí overiť, či je v súlade so zásadami dohody o spoločnosti SWIFT⁷²⁴. Po potvrdení súladu musí spoločnosť SWIFT poskytnúť finančné údaje priamo ministerstvu financií USA. Ministerstvo financií musí finančné údaje uchovávať v zabezpečenom fyzickom priestore, do ktorého majú prístup len analytici vyšetrojúci terorizmus alebo jeho financovanie a finančné údaje nesmú byť prepojené so žiadnou inou databázou. Finančné údaje získané od spoločnosti SWIFT sa vymažú najneskôr päť rokov od prijatia. Finančné údaje, ktoré sú relevantné pre osobitné vyšetrovania alebo stíhania, sa môžu uchovávať tak dlho, ako si to vyšetrovanie alebo stíhanie vyžaduje.

722 Rozhodnutie Rady 2010/412/EÚ z 13. júla 2010 o uzavretí Dohody medzi Európskou úniou a Spojenými štátmi americkými o spracovaní a zasielaní údajov obsiahnutých vo finančných správach z Európskej únie do Spojených štátov amerických na účely Programu na sledovanie financovania terorizmu, Ú. v. EÚ L 195, 2010, s. 3 a 4. Znenie tejto dohody je pripojené k tomuto rozhodnutiu, Ú. v. EÚ L 195, 2010, s. 5 – 14.

723 Tamže, článok 4 ods. 2.

724 Spoločný dozorný orgán Europolu uskutočnil audity činností Europolu v tejto oblasti.

Ministerstvo financií USA môže prenášať informácie z údajov od spoločnosti SWIFT konkrétnym orgánom presadzovania práva, verejnej bezpečnosti alebo boja proti terorizmu v USA alebo mimo USA výlučne na účely vyšetrovania, zisťovania, prevencie alebo stíhania terorizmu alebo jeho financovania. Ak ďalšie prenosy finančných údajov zahŕňajú občanov alebo osoby s trvalým pobytom v členskom štáte EÚ, každá výmena údajov s orgánmi tretej krajiny si vyžaduje predchádzajúci súhlas príslušných orgánov dotknutého členského štátu. Výnimky sú možné v prípade, že výmena údajov má zásadný význam pre prevenciu bezprostrednej a závažnej hrozby verejnej bezpečnosti.

Súlad so zásadami dohody o spoločnosti SWIFT sledujú nezávislí pozorovatelia vrátane osoby vymenovanej Európskou komisiou. Majú možnosť v reálnom čase a so spätnou účinnosťou preskúmať všetky vyhľadávania v poskytnutých údajoch, požiadať o dodatočné informácie na odôvodnenie zamerania týchto vyhľadávanií na terorizmus a oprávnenie zablokovat akékoľvek alebo všetky vyhľadávania, ktoré sa zdajú byť v rozpore so zárukami stanovenými v dohode.

Dotknuté osoby majú právo získať potvrdenie od príslušného orgánu EÚ pre ochranu údajov o dodržaní ich práv na ochranu osobných údajov. Dotknuté osoby majú tiež právo na opravu, vymazanie alebo blokovanie svojich údajov získaných a uložených ministerstvom financií USA podľa dohody o spoločnosti SWIFT. Na právo na prístup dotknutých osôb sa môžu vzťahovať určité právne obmedzenia. V prípade zamietnutia prístupu musí byť dotknutá osoba písomne informovaná o zamietnutí a o práve na správny alebo súdny prostriedok nápravy v USA.

Dohoda o spoločnosti SWIFT je účinná päť rokov, jej prvé obdobie platnosti trvalo do augusta 2015. Automaticky sa predlžuje o jeden rok, kým jedna zmluvná strana neoznámí druhej zmluvnej strane, a to v predstihu aspoň šesť mesiacov, že nemá v úmysle predĺžiť účinnosť dohody. K automatickému predĺženiu došlo v auguste 2015, 2016 a 2017 a zabezpečila sa ním platnosť dohody SWIFT aspoň do augusta 2018⁷²⁵.

725 Tamže, článok 23 ods. 2.

8

Ochrana údajov v kontexte polície a trestného súdnictva

EÚ	Zahrnuté témy	RE
Smernica o ochrane údajov pre orgány polície a trestného súdnictva	Všeobecne	Modernizovaný Dohovor č. 108
	Polícia	Odporúčanie v oblasti polície Praktická príručka o využívaní osobných údajov v policajnom sektore
	Sledovanie	ESLP, <i>B.B./Francúzsko</i> , č. 5335/06, 2009 ESLP, <i>S. a Harper/Spojené kráľovstvo [VK]</i> , č. 30562/04 a č. 30566/04, 2008 ESLP, <i>Allan/Spojené kráľovstvo</i> , č. 48539/99, 2002 ESLP, <i>Malone/Spojené kráľovstvo</i> , č. 8691/79, 1984 ESLP, <i>Klass a i./Nemecko</i> , č. 5029/71, 1978 ESLP, <i>Szabó a Vissy/Maďarsko</i> , č. 37138/14, 2016 ESLP, <i>Vetter/Francúzsko</i> , č. 59842/00, 2005
	Počítačová kriminalita	Dohovor o počítačovej kriminalite

EÚ	Zahrnuté témy	RE
Iné osobitné právne nástroje		
Prümské rozhodnutie	Osobitné údaje: odtlačky prstov, DNA, výtržníctvo, informácie o cestujúcich v leteckej doprave, telekomunikačné údaje atď.	Modernizovaný Dohovor č. 108, článok 6 Odporúčanie v oblasti polície, Praktická príručka o využívaní osobných údajov v policajnom sektore
Švédska iniciatíva (rámcové rozhodnutie Rady 2006/960/SVV)	Zjednodušenie výmeny informácií a spravodajských informácií medzi orgánmi presadzovania práva	ESLP, <i>S. a Marper/Spojené kráľovstvo</i> [VK], č. 30562/04 a č. 30566/04, 2008
Smernica (EÚ) 2016/681 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti SDEÚ, spojené veci C-293/12 a C-594/12, <i>Digital Rights Ireland a Kärntner Landesregierung a i.</i> [VK], 8. apríla 2014. SDEÚ, spojené veci C-203/15 a C-698/15, <i>Tele2 Sverige a Home Department/Tom Watson a i.</i> [VK], 2016	Uchovávanie osobných údajov	ESLP, <i>B.B./Francúzsko</i> , č. 5335/06, 2009
Nariadenie o Europol Rozhodnutie o Eurojuste	V osobitných agentúrach	Odporúčanie v oblasti polície
Rozhodnutie Schengen II Nariadenie o VIS Nariadenie Eurodac Rozhodnutie o CIS	V osobitných spoločných informačných systémoch	Odporúčanie v oblasti polície ESLP, <i>Dalea/Francúzsko</i> , č. 964/07, 2010

RE a EÚ prijali osobitné právne nástroje s cieľom vyvážiť záujmy jednotlivcov v oblasti ochrany údajov a záujmy spoločnosti pri získavaní údajov na účely boja proti trestnej činnosti a zabezpečenia národnej a verejnej bezpečnosti. V tomto oddiele sa uvádza prehľad právnych predpisov RE (oddiel 8.1) a právnych predpisov EÚ (oddiel 8.2) v súvislosti s ochranou údajov v oblasti polície a trestného súdnictva.

8.1. Právne predpisy RE o ochrane údajov a o otázkach národnej bezpečnosti, polície a trestného súdnictva

Hlavné body

- Modernizovaný Dohovor č. 108 a odporúčanie RE v oblasti polície sa týkajú ochrany údajov vo všetkých oblastiach policajnej činnosti.
- Dohovor o počítačovej kriminalite (Budapešťiansky dohovor) je záväzný medzinárodný právny nástroj, ktorý sa zaoberá trestnou činnosťou zameranou na elektronické siete a páchanou prostredníctvom elektronických sietí. Je relevantný aj pre vyšetrovanie trestných činov mimo oblasti počítačovej kriminality, ktoré zahŕňajú elektronické dôkazy.

Jedným z dôležitých rozdielov medzi právnymi predpismi RE a EÚ je, že **právne predpisy RE** sa na rozdiel od právnych predpisov EÚ vzťahujú aj na oblasť národnej bezpečnosti. Znamená to, že zmluvné strany musia podliehať pôsobnosti článku 8 ECHR aj v prípade činností súvisiacich s národnou bezpečnosťou. Viaceré rozsudky ESĽP sa týkajú činností štátu v citlivých oblastiach právnych predpisov a postupov v oblasti národnej bezpečnosti⁷²⁶.

Pokiaľ ide o oblasť polície a trestného súdnictva, modernizovaný Dohovor č. 108 sa na európskej úrovni vzťahuje na všetky oblasti spracúvania osobných údajov a jeho ustanovenia majú upravovať spracúvanie osobných údajov vo všeobecnosti. V dôsledku toho sa modernizovaný Dohovor č. 108 vzťahuje na ochranu údajov v oblasti polície a trestného súdnictva. Spracúvanie genetických údajov, osobných údajov týkajúcich sa trestných činov, trestných konaní a odsúdení a akýchkoľvek súvisiacich bezpečnostných opatrení, biometrických údajov, ktoré jednoznačne identifikujú určitú osobu, ako aj všetkých citlivých osobných údajov je povolené len vtedy, ak existujú primerané záruky vo vzťahu k rizikám, ktoré spracúvanie takýchto údajov môže predstavovať pre záujmy, práva a základné slobody dotknutej osoby; najmä pokiaľ ide o riziko diskriminácie⁷²⁷.

⁷²⁶ Pozri napríklad ESĽP, *Klass a i./Nemecko*, č. 5029/71, 6. septembra 1978; ESĽP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000 a ESĽP, *Szabó a Vissy/Maďarsko*, č. 37138/14, 12. januára 2016.

⁷²⁷ Modernizovaný Dohovor č. 108, článok 6.

Právne úlohy policajných orgánov a orgánov činných v trestnom konaní si často vyžadujú spracúvanie osobných údajov, ktoré môže mať pre dotknutých jednotlivcov vážne dôsledky. Odporúčaním v oblasti polície, ktoré RE prijala v roku 1987, sa usmerňujú členské štáty RE, pokiaľ ide o spôsob vykonávania zásad Dohovoru č. 108 v kontexte spracúvania osobných údajov policajnými orgánmi⁷²⁸. Odporúčanie bolo doplnené praktickou príručkou o využívaní osobných údajov v policajnom sektore, ktorú prijal Poradný výbor pre Dohovor č. 108⁷²⁹.

Príklad: Vo veci *D.L./Bulharsko*⁷³⁰ sociálne služby umiestnili sťažovateľku na základe súdneho príkazu do bezpečného výchovného zariadenia. Akákoľvek písomná korešpondencia a telefonické rozhovory boli predmetom plošnej a nediferencovanej kontroly zo strany inštitúcie. ESLP rozhodol, že došlo k porušeniu článku 8, keďže predmetné opatrenie nebolo nevyhnutné v demokratickej spoločnosti. ESLP konštatoval, že je potrebné urobiť všetko pre to, aby maloleté osoby umiestnené v inštitúcii mali dostatočný kontakt s vonkajším svetom, keďže predstavuje neoddeliteľnú súčasť ich práva na dôstojné zaobchádzanie a je nevyhnutný pri príprave na ich opätovné začlenenie do spoločnosti. Platí to pre návštevy, ako aj písomnú korešpondenciu alebo telefonické rozhovory. Okrem toho sa pri kontrole nerozlišovalo medzi komunikáciou s rodinnými príslušníkmi a mimovládnyimi organizáciami, ktoré zastupujú práva detí, alebo právnikmi. Rozhodnutie o zachytávaní komunikácie navyše nebolo založené na individuálnej analýze rizík v každom jednotlivom prípade.

Príklad: Vo veci *Dragojević/Chorvátsko*⁷³¹ bol sťažovateľ podozrivý z účasti na obchodovaní s drogami. Bol uznaný vinným po tom, ako vyšetrovací sudca povolil použitie opatrení tajného sledovania na odpočúvanie telefonických hovorov sťažovateľa. ESLP konštatoval, že opatrenie, ktoré je predmetom sťažnosti, predstavuje zásah do práva na rešpektovanie súkromného života a korešpondencie. Povoľenie, ktoré vydal vyšetrojúci sudca, sa zakladalo len na vyhlásení prokuratúry, že „vyšetrovanie nebolo možné vykonať inými

728 Rada Európy, Výbor ministrov (1987), Odporúčanie členským štátom Rec (87)15, ktorým sa upravuje používanie osobných údajov v policajnom sektore, 17. septembra 1987.

729 Rada Európy (2018), Poradný výbor pre Dohovor č. 108, Praktická príručka o využívaní osobných údajov v policajnom sektore, T-PD(2018)1.

730 ESLP, *D.L./Bulharsko*, č. 7472/14, 19. mája 2016.

731 ESLP, *Dragojević/Chorvátsko*, č. 68955/11, 15. januára 2015.

prostriedkami". EŠLP tiež uviedol, že trestné súdy obmedzili svoje posúdenie týkajúce sa použitia monitorovacích opatrení a že vláda neuviedla, aké prostriedky nápravy sú k dispozícii. V dôsledku toho došlo k porušeniu článku 8.

8.1.1. Odporúčanie v oblasti polície

EŠLP neustále zdôrazňuje, že uchovávanie osobných údajov políciou alebo národnými bezpečnostnými orgánmi predstavuje zasahovanie v zmysle článku 8 ods. 1 ECHR. V mnohých rozsudkoch EŠLP sa rieši otázka opodstatnenosti takýchto zásahov⁷³².

Príklad: Vo veci *B.B./Francúzsko*⁷³³ bol sťažovateľ odsúdený za spáchanie sexuálnych trestných činov na 15-ročných maloletých osobách, voči ktorým vystupoval ako dôveryhodná osoba. Výkon trestu odňatia slobody ukončil v roku 2000. O rok neskôr požiadal o odstránenie záznamu o tomto odsúdení z registra trestov, ale táto žiadosť bola zamietnutá. V roku 2004 sa podľa francúzskeho práva vytvorila vnútroštátna súdna databáza páchatelov sexuálnych trestných činov a sťažovateľ bol informovaný o svojom zaradení do tejto databázy. EŠLP rozhodol, že zahrnutie osoby odsúdenej za sexuálny trestný čin do vnútroštátnej súdnej databázy patrí do rozsahu pôsobnosti článku 8 ECHR. Vzhľadom na skutočnosť, že boli prijaté dostatočné záruky ochrany údajov, napríklad právo dotknutej osoby požiadať o vymazanie údajov, obmedzenie lehoty uchovávania údajov, ako aj obmedzenie prístupu k uvedeným údajom, dosiahla sa primeraná rovnováha medzi konkurenčnými súkromnými a verejnými záujmami. Súd dospel k záveru, že nedošlo k porušeniu článku 8 ECHR.

Príklad: Vo veci *S. a Marper/Spojené kráľovstvo*⁷³⁴ boli obaja sťažovatelia obvinení zo spáchania trestných činov, neboli však odsúdení. Polícia im napriek tomu odobrala odtlačky prstov, profily DNA a bunkové vzorky a uchovávala ich. Neobmedzené uchovávanie biometrických údajov bolo povolené ustanovením, podľa ktorého bola osoba podozrivá zo spáchania trestného

732 Pozri napríklad EŠLP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987; EŠLP, *M.M./Spojené kráľovstvo*, č. 24029/07, 13. novembra 2012; EŠLP, *M.K./Francúzsko*, č. 19522/09, 18. apríla 2013, alebo EŠLP, *Aycaguer/Francúzsko*, č. 8806/12, 22. júna 2017.

733 EŠLP, *B.B./Francúzsko*, č. 5335/06, 17. decembra 2009.

734 EŠLP, *S. a Marper/Spojené kráľovstvo* [VK], č. 30562/04 a 30566/04, 4. decembra 2008, body 119 a 125.

činu dokonca aj vtedy, keď bola neskôr zbavená obvinenia alebo prepustená. EŠLP uviedol, že paušálne a nerozlišujúce uchovávanie osobných údajov, ktoré nebolo časovo obmedzené a pri ktorom osoby zbavené podozrenia mali len obmedzené možnosti požiadať o výmaz, predstavuje neprimerané zasahovanie do práva sťažovateľov na rešpektovanie súkromného života. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Kľúčovou otázkou v kontexte elektronických komunikácií je zásah orgánov verejnej moci do práv na súkromie a ochranu údajov. Prostriedky sledovania alebo odpočúvania komunikácie, ako sú zariadenia na odpočúvanie, sú prípustné len vtedy, ak sa to stanovuje v právnom predpise a ak to predstavuje nevyhnutné opatrenie v demokratickej spoločnosti v záujme:

- ochrany bezpečnosti štátu,
- verejnej bezpečnosti,
- peňažných záujmov štátu,
- potláčania trestnej činnosti alebo
- ochrany dotknutej osoby alebo práv a slobôd iných.

V mnohých ďalších rozsudkoch EŠLP sa rieši otázka odôvodnenosti zásahu do práva na súkromie sledovaním.

Príklad: Vo veci *Allan/Spojené kráľovstvo*⁷³⁵ orgány tajne nahrávali súkromné rozhovory väzňa s jeho priateľom v miestnosti vyhradenej pre návštevy a s ďalším obvineným vo väzenskej cele. EŠLP konštatoval, že používanie zariadení na vytváranie zvukových alebo obrazových záznamov v cele sťažovateľa, vo väzenskej miestnosti pre návštevy a pri rozhovore s ďalším obvineným v cele predstavuje zasahovanie do práva sťažovateľa na súkromný život. Keďže v danom čase neexistoval žiadny zákonný systém, ktorý by políciu oprávňoval používať skryté záznamové zariadenia, zásah nebol v súlade s právnymi predpismi. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

⁷³⁵ EŠLP, *Allan/Spojené kráľovstvo*, č. 48539/99, 5. novembra 2002.

Príklad: Vo veci *Roman Zakharov/Rusko*⁷³⁶ podal sťažovateľ žalobu proti trom prevádzkovateľom mobilných sietí. Tvrdil, že jeho právo na súkromie jeho telefónnej komunikácie bolo porušené, keďže prevádzkovatelia nainštalovali zariadenie, ktoré federálnej bezpečnostnej službe umožňuje odpočúvať jeho telefonickú komunikáciu bez predchádzajúceho súdneho povolenia. EŠLP rozhodol, že vnútroštátne právne ustanovenia upravujúce odpočúvanie komunikácie neposkytujú primerané a účinné záruky pred svojvoľnosťou a rizikom zneužitia. Konkrétne, vo vnútroštátnych právnych predpisoch sa nevyžadovalo vymazanie uchovávaných údajov po tom, ako sa dosiahol účel ich uchovávaní. Navyše, hoci sa vyžadovalo povolenie súdu, súdna kontrola bola obmedzená.

Príklad: Sťažovatelia vo veci *Szabó a Vissy/Maďarsko*⁷³⁷ tvrdili, že maďarská právna úprava porušuje článok 8 ECHR, keďže nie je dostatočne podrobná ani presná. Okrem toho tvrdili, že právne predpisy neposkytujú dostatočné záruky proti zneužívaniu a svojvoľnosti. EŠLP konštatoval, že podľa maďarských právnych predpisov sa nevyžaduje, aby pri sledovaní bolo potrebné povolenie súdu. Napriek tomu súd uviedol, že hoci sledovanie podliehalo schváleniu ministra spravodlivosti, bolo výrazne politické a neschopné zabezpečiť požadované posúdenie „striktnej nevyhnutnosti“. Okrem toho sa podľa vnútroštátneho práva neumožňovalo súdne preskúmanie, keďže dotknutým osobám sa nezasielalo žiadne oznámenie. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Keďže spracúvanie údajov policajnými orgánmi môže mať významný vplyv na dotknuté osoby, je obzvlášť nutné prijať podrobné pravidlá ochrany údajov pre spracúvanie osobných údajov v tejto oblasti. Riešením tohto problému sa zaoberalo odporúčanie RE v oblasti polície, ktoré obsahuje usmernenia o spôsobe získavania údajov pre policajnú činnosť, spôsobe uchovávaní súborov s údajmi v tejto oblasti, o tom, kto by mal mať prístup k týmto súborom vrátane podmienok prenosu údajov zahraničným policajným orgánom, akým spôsobom by dotknuté osoby mali vykonávať svoje práva na ochranu údajov a ako by sa mala vykonávať kontrola nezávislými orgánmi. Zohľadňuje sa v ňom aj povinnosť zabezpečiť primeranú bezpečnosť osobných údajov.

736 EŠLP, *Roman Zakharov/Rusko*, č. 47143/06, 4. decembra 2015.

737 EŠLP, *Szabó a Vissy/Maďarsko*, č. 37138/14, 12. januára 2016.

Odporúčanie sa nevyslovuje za neobmedzené a nediferencované získavanie údajov policajnými orgánmi. Získavanie osobných údajov policajnými orgánmi obmedzuje na mieru nevyhnutne potrebnú na predchádzanie skutočnému nebezpečenstvu alebo stíhanie špecifických trestných činov. Každé dodatočné získavanie údajov by malo vychádzať z konkrétnych vnútroštátnych predpisov. Spracúvanie citlivých údajov by sa malo obmedziť na mieru, ktorá je nevyhnutne potrebná v kontexte konkrétneho vyšetrovania.

Ak sa získavajú osobné údaje bez vedomia dotknutej osoby, dotknutú osobu je nutné informovať o takomto získavaní ihneď po tom, ako toto informovanie nebude brániť vyšetrovaniu. Získavanie údajov pomocou technických prostriedkov sledovania alebo iných automatizovaných prostriedkov by tiež malo mať osobitný právny základ.

Príklad: Vo veci *Versini-Campinchi a Crasnianski/Francúzsko*⁷³⁸ sťažovateľka, ktorá bola advokátkou, vykonala telefonický rozhovor s klientom, ktorého telefónna linka bola odpočúvaná na žiadosť vyšetrojúceho sudcu. Z prepisu rozhovoru vyplynulo, že prezradila informácie, na ktoré sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť. Prokurátor zaslal túto informáciu advokátskej komore, ktorá jej uložila sankciu. ESLP uznal existenciu zásahu do práva na rešpektovanie súkromného života a korešpondencie, a to nielen osoby, ktorej telefón bol odpočúvaný, ale aj sťažovateľky, ktorej komunikácia bola odpočúvaná a prepísaná. K zásahu došlo v súlade s právnymi predpismi a sledoval legitímny cieľ predchádzania narušovaniu verejného poriadku. Sťažovateľka dosiahla preskúmanie zákonnosti predloženia prepisu telefonického záznamu v rámci disciplinárneho konania, ktoré sa voči nej začalo. Hoci sťažovateľka nemohla podať žiadosť o vyňatie zápisu telefonického rozhovoru, ESLP sa domnieval, že bola vykonaná účinná kontrola schopná obmedziť zásah, ktorého sa sťažnosť týkala, a ktorá bola potrebná v demokratickej spoločnosti. ESLP rozhodol, že tvrdenie, že možnosť trestného stíhania advokátky na základe prepisu môže mať odstrašujúci účinok na slobodu komunikácie medzi advokátkou a jeho klientom, a teda na práva na obhajobu klienta, neobstojí, ak skutočnosť, že advokátka poskytla informácie sama o sebe mohla prestavovať protiprávne konanie advokátky. V dôsledku toho sa nezistilo žiadne porušenie článku 8.

⁷³⁸ ESLP, *Versini-Campinchi a Crasnianski/Francúzsko*, č. 49176/11, 16. júna 2016.

V odporúčaní RE v oblasti polície sa stanovuje, že pri uchovávaní osobných údajov sa musia jasne rozlišovať: administratívne údaje a policajné údaje, osobné údaje rôznych kategórií dotknutých osôb, napríklad podozrivých osôb, odsúdených osôb, obetí a svedkov, ako aj údaje, ktoré treba považovať za reálne fakty, a tie, ktoré sa zakladajú na podozrení alebo domnienkach.

Účel, na ktorý sa môžu použiť policajné údaje, musí byť prísne obmedzený. Ovplyvňuje to poskytovanie policajných údajov tretím stranám: prenos alebo poskytnutie takýchto údajov v rámci policajného sektora by sa mali riadiť tým, či existuje alebo neexistuje legitímny záujem na výmene takýchto informácií. Prenos alebo poskytnutie takýchto údajov mimo policajného sektora by sa mali povoliť len vtedy, ak existuje jasný právny záväzok alebo oprávnenie.

Príklad: Vo veci *Karabeyoğlu/Turecko*⁷³⁹ boli telefónne linky sťažovateľa, ktorý bol sudcom, monitorované v rámci vyšetrovania nezákonnej organizácie, v súvislosti s ktorou bol podozrivý z toho, že je jej členom alebo že jej poskytuje pomoc a podporu. V nadväznosti na rozhodnutie nezačať trestné stíhanie prokurátor zodpovedný za vyšetrovanie zničil predmetné nahrávky. Kópia však zostala v držbe súdnych vyšetrovateľov, ktorí potom použili relevantné časti v rámci disciplinárneho konania proti sťažovateľovi. ESĽP rozhodol, že príslušné právne predpisy boli porušené, keďže informácie boli použité na iné účely ako tie, na ktoré boli získané, a neboli zničené v zákonnej lehote. Zásah do práva sťažovateľa na rešpektovanie súkromného života nebol v prípade disciplinárneho konania voči nemu v súlade s právnymi predpismi.

Medzinárodný prenos alebo poskytnutie by sa mali obmedziť na zahraničné policajné orgány a mali by sa zakladať na osobitných právnych ustanoveniach, podľa možností medzinárodných dohodách, okrem prípadov, keď sú nutné pri predchádzaní závažnému a bezprostrednému nebezpečenstvu.

Spracúvanie údajov políciou musí podliehať nezávislému dozoru s cieľom zaistiť súlad s vnútroštátnymi predpismi na ochranu údajov. Dotknuté osoby musia mať všetky práva na prístup, ktoré sa uvádzajú v modernizovanom Dohovore č. 108. V prípade, že sú práva prístupu dotknutých osôb obmedzené podľa článku 9 Dohovoru č. 108 v záujme efektívneho policajného vyšetrovania a výkonu trestných sankcií, dotknutá osoba musí mať podľa vnútroštátnych právnych predpisov právo

⁷³⁹ ESĽP, *Karabeyoğlu/Turecko*, č. 30083/10, 7. júna 2016.

na odvolanie pred národným dozorným orgánom pre ochranu údajov alebo iným nezávislým orgánom.

8.1.2. Budapešťiansky dohovor o počítačovej kriminalite

Keďže pri trestnej činnosti sa stále častejšie používajú elektronické systémy na spracúvanie údajov, ktoré ju zároveň ovplyvňujú, sú v reakcii na tento vývoj potrebné nové trestnoprávne ustanovenia. RE preto prijala medzinárodný právny nástroj – Dohovor o počítačovej kriminalite, tiež známy ako Budapešťiansky dohovor, s cieľom riešiť problém trestnej činnosti páchanej proti elektronickým sieťam a ich prostredníctvom⁷⁴⁰. Dohovor je otvorený na pristúpenie aj štátom, ktoré nie sú členmi RE. Na začiatku roka 2018 bolo stranami dohovoru 14 štátov mimo RE⁷⁴¹ a sedem ďalších štátov, ktoré nie sú členmi, bolo vyzvaných na pristúpenie.

Dohovor o počítačovej kriminalite je stále najvplyvnejšou medzinárodnou zmluvou, ktorou sa upravuje porušenie právnych predpisov týkajúcich sa internetu alebo iných informačných sietí. Vyžaduje sa v ňom, aby strany aktualizovali a harmonizovali svoje trestnoprávne predpisy proti hackerstvu a ďalším porušeniam bezpečnosti vrátane porušovania autorských práv, podvodov s využitím výpočtovej techniky, detskej pornografie a ďalších nezákonných počítačových činností. V Dohovore sa takisto stanovujú procesné právomoci týkajúce sa vyhľadávania v počítačových sieťach a odpočúvania komunikácie v kontexte boja proti počítačovej kriminalite. Umožňuje aj účinnú medzinárodnú spoluprácu. Dodatočným protokolom k Dohovoru sa upravuje kriminalizácia rasistickej a xenofóbnej propagandy v počítačových sieťach.

Dohovor síce nie je nástrojom na podporu ochrany údajov, kriminalizujú sa ním však činnosti, ktorými sa pravdepodobne porušia práva dotknutých osôb na ochranu údajov. Okrem toho sa v ňom vyžaduje, aby zmluvné strany prijali legislatívne opatrenia, ktoré umožnia ich vnútroštátnym orgánom zachytávať prevádzkové a obsahové údaje⁷⁴². Dohovorom sa zmluvným stranám ukladá, aby pri jeho vykonávaní

740 Rada Európy, Výbor ministrov (2001), Dohovor o počítačovej kriminalite, CETS č. 185, Budapešť, 23. novembra 2001, nadobudol účinnosť 1. júla 2004.

741 Austrália, Čile, Dominikánska republika, Izrael, Japonsko, Kanada, Kolumbia, Maurícius, Panama, Senegal, Spojené štáty, Srí Lanka, Tonga, a Tunisko. Pozri [Chart of signatures and ratifications of Treaty 185](#), stav k júlu 2017.

742 Rada Európy, Výbor ministrov (2001), Dohovor o počítačovej kriminalite, CETS č. 185, Budapešť, 23. novembra 2001, články 20 a 21.

zohľadnili primeranú ochranu ľudských práv a slobôd vrátane práv zaručených ECHR, napríklad práva na ochranu údajov⁷⁴³. Zmluvné strany nie sú povinné pristúpiť aj k Dohovoru č. 108, aby mohli pristúpiť k Budapešťanskemu dohovoru o počítačovej kriminalite.

8.2. Právne predpisy EÚ o ochrane údajov v oblasti polície a trestného súdnictva

Hlavné body

- Ochrana údajov v oblasti polície a trestného súdnictva je v rámci EÚ regulovaná v kontexte vnútroštátneho aj cezhraničného spracúvania údajov zo strany policajných orgánov a orgánov trestného súdnictva členských štátov a aktérov EÚ.
- Na úrovni členských štátov je potrebné začleniť do vnútroštátnych právnych predpisov smernicu o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní.
- Osobitnými právnymi nástrojmi sa upravuje ochrana údajov v rámci cezhraničnej spolupráce v oblasti polície a presadzovania práva, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti.
- Osobitné režimy ochrany údajov existujú pre Európsky policajný úrad (Europol) a Európsku jednotku pre justičnú spoluprácu (Eurojust), čo sú orgány EÚ, ktoré pomáhajú pri cezhraničnom presadzovaní práva a podporujú ho.
- Osobitné režimy ochrany údajov takisto existujú pre spoločné informačné systémy, ktoré boli zriadené na úrovni EÚ na účely cezhraničnej výmeny informácií medzi príslušnými policajnými a súdnymi orgánmi. Dôležitými príkladmi sú Schengenský informačný systém II (SIS II), vízový informačný systém (VIS) a Eurodac – centralizovaný systém obsahujúci údaje o odtlačkoch prstov štátnych príslušníkov tretích krajín a osôb bez štátnej príslušnosti žiadajúcich o azyl v niektorom z členských štátov EÚ.
- EÚ aktualizuje uvedené ustanovenia o ochrane údajov, aby boli v súlade s ustanoveniami smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní.

743 Tamže, článok 15 ods. 1.

8.2.1. Smernica o ochrane údajov pre orgány polície a trestného súdnictva

Cieľom smernice (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov (smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní)⁷⁴⁴ je ochrana osobných údajov získaných a spracúvaných na účely trestného súdnictva, ako je:

- predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo výkon trestných sankcií vrátane ochrany pred ohrozeniami verejnej bezpečnosti a predchádzania týmto ohrozeniam,
- výkon trestnej sankcie a
- v prípadoch, keď policajné orgány alebo iné orgány presadzovania práva konajú s cieľom dodržať zákon a chrániť pred ohrozením verejnej bezpečnosti a základných práv spoločnosti a predchádzať takémuto ohrozeniu, ktoré by mohlo predstavovať trestný čin.

Smernicou o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sa chránia osobné údaje rôznych kategórií osôb zapojených do trestného konania, napríklad svedkov, informátorov, obetí, podozrivých a spolupáchateľov. Policajné orgány a orgány činné v trestnom konaní sú povinné dodržiavať ustanovenia smernice vždy, keď spracúvajú takéto osobné údaje na účely presadzovania práva, a to v rámci osobnej aj vecnej pôsobnosti smernice⁷⁴⁵.

Za určitých podmienok je však povolené aj použitie údajov na iný účel. Spracúvanie údajov na iný účel presadzovania práva ako ten účel, na ktorý sa osobné údaje získavajú, je povolené, len pokiaľ je zákonné, nevyhnutné a primerané podľa vnútroštátneho práva alebo práva EÚ⁷⁴⁶. Pri iných účeloch sa uplatňujú pravidlá všeobec-

⁷⁴⁴ Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, Ú. v. EÚ L 119, 2016, s. 89 (smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní).

⁷⁴⁵ Smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, článok 2 ods. 1.

⁷⁴⁶ Tamže, článok 4 ods. 2.

ného nariadenia o ochrane údajov. Logovanie a dokumentovanie výmeny údajov je jednou z osobitných povinností príslušných orgánov s cieľom pomáhať pri objasňovaní povinností vyplývajúcich zo sťažností.

Príslušné orgány pôsobiace v oblasti polície a trestného súdnictva sú orgány verejnej moci alebo orgány oprávnené na základe vnútroštátneho práva a verejných právomocí vykonávať funkcie orgánov verejnej moci⁷⁴⁷, napr. súkromné väznice⁷⁴⁸. Smernica sa uplatňuje tak na spracúvanie údajov na vnútroštátnej úrovni, ako aj na cezhraničné spracúvanie medzi policajnými a justičnými orgánmi členských štátov, ako aj na medzinárodné prenosy príslušnými orgánmi do tretích krajín a medzinárodným organizáciám⁷⁴⁹. Nevzťahuje sa na národnú bezpečnosť ani na spracúvanie osobných údajov inštitúciami, orgánmi, úradmi a agentúrami EÚ⁷⁵⁰.

Smernica sa vo veľkej miere opiera o zásady a definície obsiahnuté vo všeobecnom nariadení o ochrane údajov, pričom zohľadňuje osobitnú povahu oblasti polície a trestného súdnictva. Dohľad môžu vykonávať tie isté orgány členského štátu, ktoré ho vykonávajú podľa všeobecného nariadenia o ochrane údajov. V smernici sa k novým povinnostiam pre policajné orgány a orgány činné v trestnom konaní pridáva určenie zodpovednej osoby a vykonávanie posúdení vplyvu na ochranu údajov⁷⁵¹. Hoci tieto pojmy vychádzajú zo všeobecného nariadenia o ochrane údajov, smernica sa zaoberá osobitnou povahou policajných orgánov a orgánov činných v trestnom konaní. V porovnaní so spracúvaním údajov na komerčné účely, ktoré sa upravuje nariadením, si môže spracúvanie v oblasti bezpečnosti vyžadovať určitú mieru flexibility. Napríklad poskytnutie rovnakej úrovne ochrany pre dotknutú osobu, pokiaľ ide o právo na informácie, prístup k osobným údajom alebo ich vymazanie, ako sa uvádza v rámci všeobecného nariadenia o ochrane údajov, by mohlo znamenať, že akákoľvek činnosť sledovania vykonávaná na účely presadzovania práva by v kontexte presadzovania práva bola neúčinná. V smernici sa preto nespomína zásada transparentnosti. Rovnako zásady minimalizácie údajov a obmedzenia účelu, pri ktorých sa vyžaduje, aby sa osobné údaje obmedzili len na to, čo je

747 Tamže, článok 3 ods. 7.

748 Európska komisia (2016), oznámenie Komisie Európskemu parlamentu podľa článku 294 ods. 6 Zmluvy o fungovaní Európskej únie o pozícii Rady k prijatiu smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stihania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov, ktorou sa zrušuje rámcové rozhodnutie Rady 2008/977/SVV, COM(2016) 213 final, Brusel, 11. apríla 2016.

749 Smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, kapitola V.

750 Tamže, článok 2 ods. 3.

751 Tamže, v článku 32 a článku 27.

nevyhnutné vzhľadom na účely, na ktoré sa spracúvajú, a ktoré sa majú spracúvať na konkrétne a výslovne uvedené ciele, sa musia pri spracúvaní v oblasti bezpečnosti uplatňovať flexibilnejšie. Informácie, ktoré príslušné orgány získavajú a uchovávajú v konkrétnom prípade, môžu byť mimoriadne užitočné pri riešení budúcich prípadov.

Zásady týkajúce sa spracúvania

V smernici o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sa stanovujú niektoré kľúčové záruky týkajúce sa používania osobných údajov. Uvádzajú sa aj zásady, ktorými sa riadi spracúvanie týchto údajov. Členské štáty musia zabezpečiť, aby osobné údaje boli:

- spracúvané zákonným spôsobom a spravodlivo,
- získané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú byť spracúvané spôsobom, ktorý je nezlučiteľný s týmito účelmi,
- primerané, relevantné a nie neúmerne vo vzťahu k účelom, na ktoré sa spracúvajú,
- správne a podľa potreby aktualizované; musia sa vykonať všetky potrebné kroky, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia;
- uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa spracúvajú,
- spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, likvidáciou alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení⁷⁵².

Podľa tejto smernice je spracúvanie zákonné iba vtedy, ak sa uskutočňuje v rozsahu potrebnom na vykonanie príslušnej úlohy. Okrem toho by ho mal vykonávať príslušný orgán pri plnení cieľov stanovených v smernici a malo by byť založené na

⁷⁵² Tamže, článok 4 ods. 1.

práve Únie alebo na vnútroštátnych právnych predpisoch⁷⁵³. Údaje sa nesmú uchovávať dlhšie, ako je nevyhnutné, a musia sa vymazať alebo pravidelne preskúmať v rámci určitých lehôt. Musí ich používať len príslušný orgán, a to na účel, na ktorý údaje boli získané, poskytnuté alebo sprístupnené.

Práva dotknutých osôb

V smernici sa stanovujú aj práva dotknutej osoby. Zahŕňajú:

- Právo na informácie. Členské štáty musia prevádzkovateľovi uložiť povinnosť sprístupniť dotknutej osobe: 1. totožnosť a kontaktné údaje prevádzkovateľa, 2. kontaktné údaje zodpovednej osoby, 3. účely spracúvania, na ktoré sú osobné údaje určené, 4. právo podať sťažnosť dozornému orgánu a kontaktné údaje dozorného orgánu, 5. právo na prístup k osobným údajom, právo na ich opravu alebo vymazanie a obmedzenie spracúvania údajov⁷⁵⁴. Okrem týchto všeobecných požiadaviek na informácie s v smernici stanovuje, že v osobitných prípadoch a s cieľom umožniť výkon ich práv musia prevádzkovatelia poskytnúť dotknutým osobám informácie o právnom základe spracúvania a o tom, ako dlho sa budú údaje uchovávať. Ak sa majú osobné údaje poskytnúť iným príjemcom, a to aj v tretích krajinách alebo medzinárodných organizáciách, dotknuté osoby musia byť informované o kategóriách takýchto príjemcov. Napokon, prevádzkovatelia musia poskytnúť akékoľvek ďalšie informácie s prihliadnutím na osobitné okolnosti, za ktorých sa údaje spracúvajú – napríklad, keď sa osobné údaje získali počas tajného sledovania, t. j. bez vedomia dotknutej osoby. Zaručuje sa tým spravodlivé spracúvanie vo vzťahu k dotknutej osobe⁷⁵⁵.
- Právo na prístup k osobným údajom. Členské štáty musia zabezpečiť, aby dotknutá osoba mala právo vedieť, či sa jej osobné údaje spracúvajú. Ak sa spracúvajú, dotknutá osoba by mala mať prístup k určitým informáciám, ako sú kategórie spracúvaných údajov⁷⁵⁶. Toto právo však môže byť obmedzené, napríklad, aby sa zabránilo mareniu vyšetrovania alebo aby sa zabránilo ohrozeniu stíhania trestného činu, alebo aby sa ochránila verejná bezpečnosť a práva a slobody iných⁷⁵⁷.

753 Tamže, článok 8.

754 Tamže, článok 13 ods. 1.

755 Tamže, článok 13 ods. 2.

756 Tamže, článok 14.

757 Tamže, článok 15.

- Právo na opravu osobných údajov. Členské štáty sú povinné zabezpečiť, že dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje. Okrem toho má dotknutá osoba aj právo na doplnenie neúplných osobných údajov⁷⁵⁸.
- Právo na vymazanie osobných údajov a obmedzenie spracúvania. V určitých prípadoch musí prevádzkovateľ vymazať osobné údaje. Dotknutá osoba môže okrem toho zabezpečiť vymazanie svojich osobných údajov, ale len vtedy, keď sa spracúvajú nezákonne⁷⁵⁹. V určitých situáciách môže byť namiesto vymazania obmedzené spracúvanie osobných údajov. K tomu môže dôjsť v prípadoch, keď 1. správnosť osobných údajov bola napadnutá a ich správnosť alebo nesprávnosť nemožno určiť, alebo 2. osobné údaje sú potrebné na účely dokazovania⁷⁶⁰.

Keď prevádzkovateľ odmietne opraviť alebo vymazať osobné údaje alebo obmedziť spracúvanie údajov, dotknutá osoba musí byť o tom písomne informovaná. Členské štáty môžu obmedziť toto právo na informácie aby, okrem iného, chránili verejnú bezpečnosť alebo práva a slobody iných, a to z rovnakých dôvodov ako pri obmedzení práva na prístup⁷⁶¹.

Dotknutá osoba má obvykle právo na informácie o spracúvaní svojich osobných údajov a má právo na prístup, opravu, vymazanie alebo obmedzenie spracúvania, ktoré môže vykonať priamo u prevádzkovateľa. Podľa smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní je možný aj nepriamy výkon práv dotknutých osôb prostredníctvom dozorného orgánu pre ochranu údajov, ktorý sa uplatňuje, keď prevádzkovateľ obmedzí právo dotknutej osoby⁷⁶². V článku 17 smernice sa vyžaduje, aby členské štáty prijali opatrenia, ktorými sa zabezpečí, aby sa práva dotknutých osôb mohli vykonávať aj prostredníctvom ich dozorného orgánu. Preto prevádzkovateľ musí dotknutú osobu informovať o možnosti nepriameho prístupu.

758 Tamže, článok 16 ods. 1.

759 Tamže, článok 16 ods. 2.

760 Tamže, článok 16 ods. 3.

761 Tamže, článok 16 ods. 4.

762 Tamže, článok 17.

Povinnosti prevádzkovateľa a sprostredkovateľa

V kontexte smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sú prevádzkovatelia údajov príslušnými orgánmi verejnej moci alebo inými subjektmi s príslušnou verejnou mocou a verejnými právomocami, ktoré určujú účely a prostriedky spracúvania osobných údajov. V smernici sa stanovuje niekoľko povinností pre prevádzkovateľov s cieľom zabezpečiť vysokú úroveň ochrany osobných údajov spracúvaných na účely presadzovania práva.

Príslušné orgány musia uchovávať logy o spracovateľských operáciách, ktoré vykonávajú, v systémoch automatizovaného spracúvania. Logy sa musia uchovávať aspoň o získavaní, zmene, prehliadaní, poskytovaní vrátane prenosov, kombinovaní a vymazaní osobných údajov⁷⁶³. V smernici sa stanovuje, že z logov o prehliadaní a poskytovaní musí byť možné určiť dátum a čas takýchto operácií, ich odôvodnenie, a pokiaľ možno aj identifikačné údaje osoby, ktorá tieto osobné údaje prehliadala alebo ich poskytovala, ako aj totožnosť príjemcov takýchto osobných údajov. Logy sa využijú výlučne na overovanie zákonnosti spracúvania, vlastné monitorovanie, na zabezpečenie integrity a bezpečnosti osobných údajov a na účely trestného konania⁷⁶⁴. Prevádzkovateľ a sprostredkovateľ na požiadanie sprístupnia logy dozornému orgánu.

Existuje najmä všeobecná povinnosť prevádzkovateľov prijať vhodné technické a organizačné opatrenia, aby zabezpečili, že spracúvanie sa vykonáva v súlade so smernicou, a boli schopní preukázať zákonnosť takéhoto spracúvania⁷⁶⁵. Pri navrhovaní týchto opatrení musia zohľadniť povahu, rozsah, kontext spracúvania, a čo je dôležité, akékoľvek potenciálne riziká pre práva a slobody fyzických osôb. Prevádzkovatelia by mali prijať interné pravidlá a zaviesť opatrenia, ktoré uľahčia dodržiavanie zásad ochrany údajov, najmä zásadu špecificky navrhutej a štandardnej ochrany údajov⁷⁶⁶. Ak je pravdepodobné, že spracúvanie povedie k vysokému riziku pre práva jednotlivcov – napríklad z dôvodu používania nových technológií – prevádzkovatelia musia pred začatím spracúvania vykonať posúdenie vplyvu na ochranu údajov⁷⁶⁷. V smernici sa uvádzajú aj opatrenia, ktoré musia prevádzkovatelia vykonať na zaistenie bezpečnosti spracúvania. Patria medzi ne opatrenia na

763 Tamže, článok 25 ods. 1.

764 Tamže, článok 25 ods. 2.

765 Tamže, článok 19.

766 Tamže, článok 20.

767 Tamže, článok 27.

zabránenie neoprávnenému prístupu k osobným údajom, ktoré spracúvajú, s cieľom zabezpečiť, aby oprávnené osoby mali prístup len k osobným údajom, na ktoré sa vzťahuje ich povolenie na prístup, aby funkcie systému spracúvania riadne fungovali a aby sa uchovávané osobné údaje nemohli v prípade poruchy systému poškodiť⁷⁶⁸. Ak dôjde k porušeniu ochrany osobných údajov, prevádzkovatelia do troch dní musia informovať dozorný orgán, pričom opíšu povahu porušenia, jeho pravdepodobné následky, kategórie príslušných osobných údajov a približný počet dotknutých osôb, ktorých sa porušenie týka. Porušenie ochrany osobných údajov sa musí oznámiť aj dotknutej osobe, a to „bez zbytočného odkladu“, ak je pravdepodobné, že porušenie povedie k vysokému riziku pre jej práva a slobody⁷⁶⁹.

Smernica obsahuje zásadu zodpovednosti, v súlade s ktorou sa ukladá prevádzkovateľom povinnosť vykonávať opatrenia na zabezpečenie dodržiavania tejto zásady. Prevádzkovatelia musia viesť záznamy o všetkých kategóriách spracovateľských činností, za ktoré sú zodpovední: podrobný obsah týchto záznamov je uvedený v článku 24 smernice. Záznamy sa na požiadanie sprístupnia dozornému orgánu, aby mohol monitorovať spracovateľské operácie prevádzkovateľa. Ďalším dôležitým opatrením na zvýšenie zodpovednosti je určenie zodpovednej osoby. Prevádzkovatelia musia určiť zodpovednú osobu, hoci podľa smernice sa členským štátom umožňuje oslobodiť od tejto povinnosti súdy a iné nezávislé justičné orgány⁷⁷⁰. Povinnosti zodpovednej osoby sa podobajú povinnostiam zodpovednej osoby podľa všeobecného nariadenia o ochrane údajov. Monitoruje dodržiavanie smernice, poskytuje informácie a poskytuje poradenstvo zamestnancom, ktorí vykonávajú spracúvanie údajov, o ich povinnostiach podľa právnych predpisov o ochrane údajov. Zodpovedná osoba poskytuje poradenstvo o potrebe vykonať posúdenie vplyvu na ochranu údajov a slúži ako kontaktné miesto pre dozorný orgán.

Prenosy do tretích krajín alebo medzinárodným organizáciám

Podobne ako vo všeobecnom nariadení o ochrane údajov, aj v smernici sa stanovujú podmienky prenosu osobných údajov do tretích krajín alebo medzinárodným organizáciám. Ak by sa osobné údaje prenášali voľne mimo jurisdikcie EÚ, záruky a silná ochrana poskytovaná podľa práva EÚ by sa mohli oslabiť. Samotné podmienky sú však dosť odlišné od podmienok vo všeobecnom nariadení o ochrane údajov. Prenos

⁷⁶⁸ Tamže, článok 29.

⁷⁶⁹ Tamže, článok 30 a 31.

⁷⁷⁰ Tamže, článok 32.

osobných údajov do tretích krajín alebo medzinárodným organizáciám je povolený, ak⁷⁷¹:

- Prenos je potrebný na dosiahnutie cieľov smernice.
- Osobné údaje sa prenášajú príslušnému orgánu (v zmysle smernice) v tretej krajine alebo medzinárodnej organizácii – hoci v jednotlivých a osobitných prípadoch existuje výnimka z tohto pravidla⁷⁷².
- Prenos osobných údajov získaných v rámci cezhraničnej spolupráce do tretích krajín alebo medzinárodným organizáciám si vyžaduje povolenie členského štátu, z ktorého údaje pochádzajú, hoci v naliehavých prípadoch existujú výnimky.
- Európska komisia prijala rozhodnutie o primeranosti, zaviedli sa primerané záruky alebo sa uplatňuje výnimka pre prenosi v osobitných situáciách.
- Následný prenos osobných údajov do inej tretej krajiny alebo medzinárodnej organizácii si vyžaduje predchádzajúce povolenie príslušného orgánu, od ktorého údaje pochádzajú, ktorý zohľadní okrem iného závažnosť trestného činu a úroveň ochrany údajov v cieľovej krajine druhého medzinárodného prenosu⁷⁷³.

Podľa tejto smernice sa prenosi osobných údajov môžu uskutočniť, ak je splnená jedna z troch podmienok. Po prvé, keď Európska komisia vydala rozhodnutie o primeranosti podľa smernice. Toto rozhodnutie sa môže vzťahovať na celé územie tretej krajiny alebo na konkrétne odvetvia tretej krajiny, alebo na medzinárodnú organizáciu. Do úvahy to však prichádza len vtedy, ak je zabezpečená primeraná úroveň ochrany a sú splnené podmienky stanovené v smernici⁷⁷⁴. V takýchto prípadoch sa na prenos osobných údajov nevyžaduje povolenie členského štátu⁷⁷⁵. Európska komisia musí monitorovať vývoj, ktorý by mohol ovplyvniť pôsobenie rozhodnutí o primeranosti. Okrem toho musí rozhodnutie obsahovať mechanizmus pravidelného preskúmania. Komisia môže tiež zrušiť, zmeniť alebo pozastaviť rozhodnutie na základe dostupných informácií o tom, že podmienky v tretej krajine alebo

771 Tamže, článok 35.

772 Tamže, článok 39.

773 Tamže, článok 35 ods. 1.

774 Tamže, článok 36.

775 Tamže, článok 36 ods. 1.

medzinárodnej organizácii už nezabezpečujú primeranú úroveň ochrany. Ak áno, Komisia musí začať konzultácie s treťou krajinou alebo s medzinárodnou organizáciou s cieľom napraviť túto situáciu.

Ak neexistuje rozhodnutie o primeranosti, prenosy sa môžu zakladať na primeraných zárukách. Môžu byť stanovené v právne záväznom akte alebo prevádzkovateľ môže vykonať vlastné posúdenie okolností sprevádzajúcich prenos osobných údajov a dospieť k záveru, že existujú primerané záruky. Pri vlastnom posúdení by sa mali zohľadniť možné dohody o spolupráci uzatvorené medzi Europolom alebo Eurojustom a treťou krajinou alebo medzinárodnou organizáciou, existencia povinností zachovania dôvernosti a obmedzenie účelu, ako aj poskytnuté záruky, že sa tieto údaje nepoužijú v žiadnej forme krutého alebo neľudského zaobchádzania vrátane trestu smrti⁷⁷⁶. V poslednom uvedenom prípade musí prevádzkovateľ informovať príslušný dozorný orgán o kategóriách prenosov v rámci tejto kategórie⁷⁷⁷.

V prípadoch, keď nebolo prijaté žiadne rozhodnutie o primeranosti alebo sa nestanovili primerané záruky, sa prenosy môžu povoliť v osobitných situáciách uvedených v smernici. Tie zahŕňajú okrem iného ochranu životne dôležitých záujmov dotknutej osoby alebo inej osoby a predchádzanie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti členského štátu alebo tretej krajiny⁷⁷⁸.

V jednotlivých a osobitných prípadoch môžu príslušné orgány uskutočňovať prenosy príjemcom usadeným v tretích krajinách, ktoré nie sú príslušnými orgánmi, ak, okrem jednej z troch opísaných podmienok, sú splnené aj dodatočné podmienky stanovené v článku 39 smernice. Prenos musí byť najmä úplne nevyhnutný na plnenie úlohy príslušného orgánu, ktorý prenos uskutočňuje a ktorý je tiež zodpovedný za určenie toho, že žiadne základné práva alebo slobody jednotlivcov neprevažujú nad verejným záujmom, ktorým je prenos odôvodnený. Takéto prenosy sa musia zdokumentovať a príslušný dozorný orgán, ktorý prenos uskutočňuje, musí informovať príslušný dozorný orgán⁷⁷⁹.

Napokon, pokiaľ ide o tretie krajiny a medzinárodné organizácie, v smernici sa tiež vyžaduje vytváranie mechanizmov medzinárodnej spolupráce na uľahčenie

⁷⁷⁶ Tamže, odôvodnenie 71.

⁷⁷⁷ Tamže, článok 37 ods. 1.

⁷⁷⁸ Tamže, článok 38 ods. 1.

⁷⁷⁹ Tamže, článok 37 ods. 3.

účinného presadzovania právnych predpisov, čím sa dozorným orgánom pre ochranu údajov pomáha pri spolupráci s ich zahraničnými partnermi⁷⁸⁰.

Nezávislý dozor a prostriedky nápravy pre dotknuté osoby

Každý členský štát musí zabezpečiť, aby jeden alebo viaceré nezávislé národné dozorné orgány boli zodpovedné za poradenstvo a monitorovanie uplatňovania ustanovení prijatých podľa tejto smernice⁷⁸¹. Dozorný orgán zriadený na účely tejto smernice môže byť totožný s dozorným orgánom zriadeným podľa všeobecného nariadenia o ochrane údajov, členské štáty však môžu určiť iný orgán za predpokladu, že spĺňa kritériá nezávislosti. Dozorné orgány sa zaoberajú aj sťažnosťami, ktoré podala akákoľvek osoba, pokiaľ ide o ochranu jej práv a slobôd v súvislosti so spracúvaním osobných údajov príslušnými orgánmi.

Ak sa výkon práv dotknutej osoby odmietne zo závažných dôvodov, dotknutá osoba musí mať právo odvolať sa na príslušný národný dozorný orgán a/alebo súd. Ak osoba utrpí ujmu v dôsledku porušenia vnútroštátneho práva, ktorým sa vykonáva smernica, má nárok na náhradu škody od prevádzkovateľa alebo akéhokoľvek iného orgánu príslušného podľa práva členského štátu⁷⁸². Dotknuté osoby vo všeobecnosti musia mať prístup k súdnemu prostriedku nápravy pri každom porušení ich práv zaručených vnútroštátnymi právnymi predpismi, ktorými sa vykonáva smernica⁷⁸³.

8.3. Iné osobitné právne nástroje týkajúce sa ochrany údajov v oblasti presadzovania práva

Výmena informácií uchovávaných členskými štátmi v špecifických oblastiach je okrem smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní upravená viacerými právnymi nástrojmi, napríklad rámcovým rozhodnutím Rady 2009/315/SVV o organizácii a obsahu výmeny informácií z registra trestov medzi členskými štátmi, rozhodnutím Rady upravujúcim spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov, a rámcovým rozhodnutím Rady 2006/960/SVV o zjednodušení výmeny informácií

780 Tamže, článok 40.

781 Tamže, článok 41.

782 Tamže, článok 56.

783 Tamže, článok 54.

a spravodajských informácií medzi orgánmi členských štátov Európskej únie činnými v trestnom konaní⁷⁸⁴.

Je dôležité, že cezhraničná spolupráca⁷⁸⁵ medzi príslušnými orgánmi stále častejšie zahŕňa výmenu údajov o prístahovateľoch. Táto právna oblasť nepatrí k záležitostiam polície a trestného súdnictva, ale z viacerých hľadísk sa týka činnosti policajných a súdnych orgánov. To isté platí pre údaje o tovare, ktorý sa dováža do EÚ alebo vyváža z EÚ. Odstránením kontrol na vnútorných hraniciach v rámci schengenského priestoru sa zvýšilo riziko podvodu, čo viedlo k zintenzívneniu spolupráce členských štátov, najmä prostredníctvom rozšírenia cezhraničnej výmeny informácií, s cieľom účinnejšie odhaľovať a stíhať porušenia vnútroštátnych a európskych colných predpisov. Okrem toho sa v posledných rokoch vo svete zaznamenal nárast závažnej a organizovanej trestnej činnosti a terorizmu, čo môže zahŕňať medzinárodné cestovanie, a v mnohých prípadoch sa objavila potreba zvýšenej cezhraničnej spolupráce policajných orgánov a orgánov presadzovania práva.⁷⁸⁶

Prümské rozhodnutie

Dôležitým príkladom inštitucionalizovanej cezhraničnej spolupráce formou výmeny údajov uchovávaných v členských štátoch je rozhodnutie Rady 2008/615/SVV, spolu s jeho vykonávacími ustanoveniami v rozhodnutí 2008/615/JHA o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti (prümské rozhodnutie), ktorým bola v roku 2008 zahrnutá do európskych právnych predpisov Prümská zmluva⁷⁸⁷. Prümská zmluva bola medzinárodná dohoda o poli-

784 Rada Európskej únie (2009), rámcové rozhodnutie Rady 2009/315/SVV z 26. februára 2009 o organizácii a obsahu výmeny informácií z registra trestov medzi členskými štátmi, Ú. v. EÚ L 93; Rada Európskej únie (2000), rozhodnutie Rady 2000/642/SVV zo 17. októbra 2000 upravujúce spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov, Ú. v. ES L 271; rámcové rozhodnutie Rady 2006/960/SVV z 18. decembra 2006 o zjednodušení výmeny informácií a spravodajských informácií medzi orgánmi členských štátov Európskej únie činnými v trestnom konaní, Ú. v. EÚ L 386.

785 Európska komisia (2012), *oznámenie Komisie Európskemu parlamentu a Rade – Posilnenie spolupráce v oblasti presadzovania práva v EÚ: európsky model výmeny informácií (EIXM)*, COM(2012) 735 final, Brusel, 7. decembra 2012.

786 Pozri Európska komisia (2011), návrh smernice Európskeho parlamentu a Rady o využívaní údajov z osobných záznamov o cestujúcich na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti, KOM(2011) 32 v konečnom znení, Brusel, 2. februára 2011, s. 1.

787 Rada Európskej únie (2008), rozhodnutie Rady 2008/615/SVV z 23. júna 2008 o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti, Ú. v. EÚ L 210, 2008.

cajnej spolupráci, ktorú v roku 2005 podpísali Belgicko, Francúzsko, Holandsko, Luxembursko, Nemecko, Rakúsko a Španielsko⁷⁸⁸.

Cieľom prümského rozhodnutia je pomôcť signatárskym členským štátom zlepšiť výmenu informácií na účely predchádzania trestnej činnosti a boja proti nej v troch oblastiach: terorizmus, cezhraničná trestná činnosť a nelegálna migrácia. Na tento účel rozhodnutie obsahuje ustanovenia, ktoré sa týkajú:

- automatizovaného prístupu k profilom DNA, údajom o odtlačkoch prstov a určitým údajom o vnútroštátnej registrácii vozidiel,
- poskytovania údajov v súvislosti s významnými udalosťami, ktoré majú cezhraničný rozmer,
- poskytovania informácií s cieľom zabrániť teroristickým trestným činom,
- ďalších opatrení na zintenzívnenie cezhraničnej policajnej spolupráce.

Databázy sprístupnené na základe prümského rozhodnutia sú v plnom rozsahu upravené vnútroštátnymi právnymi predpismi, výmena údajov je však dodatočne upravená rozhodnutím, ktorého zlučiteľnosť so smernicou o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sa bude musieť posúdiť. Príslušnými orgánmi dozeraúcimi na tieto toky údajov sú národné dozorné orgány pre ochranu údajov.

Rámcové rozhodnutie 2006/960/SVV – švédska iniciatíva

Rámcové rozhodnutie 2006/960/SVV (švédska iniciatíva)⁷⁸⁹ predstavuje ďalší príklad cezhraničnej spolupráce, pokiaľ ide o výmenu údajov na vnútroštátnej úrovni medzi orgánmi presadzovania práva. Švédska iniciatíva sa osobitne zameriava na výmenu spravodajských informácií a informácií a v jej článku 8 sa stanovujú osobitné pravidlá ochrany údajov.

⁷⁸⁸ Zmluva medzi Belgickým kráľovstvom, Spolkovou republikou Nemecko, Španielskym kráľovstvom, Francúzskou republikou, Luxemburským veľkovevodstvom, Holandským kráľovstvom a Rakúskou republikou o zintenzívnení cezhraničnej spolupráce najmä v boji proti terorizmu, cezhraničnej trestnej činnosti a nelegálnej migrácii.

⁷⁸⁹ Rada Európskej únie (2006), Rámcové rozhodnutie Rady 2006/960/SVV z 18. decembra 2006 o zjednodušení výmeny informácií a spravodajských informácií medzi orgánmi členských štátov Európskej únie činnými v trestnom konaní, Ú. v. EÚ L 386, 29.12.2006, s. 89.

Podľa tohto aktu použitie vymieňaných informácií a spravodajských informácií musí podliehať vnútroštátnym ustanoveniam o ochrane údajov členského štátu, ktorý informácie prijíma, v súlade s rovnakými pravidlami, ako keby informácie boli získané v tomto členskom štáte. V článku 8 sa ďalej uvádza, že príslušný orgán presadzovania práva môže pri poskytovaní informácií a spravodajských informácií uložiť podľa svojho vnútroštátneho práva prijímajúcemu orgánu presadzovania práva podmienky na použitie týchto informácií. Tieto podmienky sa môžu uplatňovať aj na podávanie správ o výsledkoch vyšetrovania trestných činov alebo na spravodajské operácie v trestných veciach, pri ktorých sa vyžadovala výmena informácií a spravodajských informácií. Ak sa však vo vnútroštátnom práve stanovujú výnimky z obmedzení používania (napr. pre súdne orgány, zákonodarné orgány atď.), informácie a spravodajské informácie sa môžu použiť len po predchádzajúcej konzultácii s poskytujúcim členským štátom.

Poskytnuté informácie a spravodajské informácie sa môžu použiť:

- na účely, na ktoré boli poskytnuté,
- na zabránenie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti.

Spracúvanie na iné účely môže byť povolené, ale len na základe predchádzajúceho povolenia poskytujúceho členského štátu.

V švédskej iniciatíve sa ďalej uvádza, že spracúvané osobné údaje musia byť chránené v súlade s medzinárodnými nástrojmi, ako sú:

- Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov⁷⁹⁰,
- Dodatkový protokol z 8. novembra 2001 k tomuto Dohovoru týkajúceho sa dozorných orgánov a cezhraničných tokov údajov⁷⁹¹,
- odporúčanie Rady Európy R(87) 15, ktorým sa upravuje používanie osobných údajov v policajnom sektore⁷⁹².

790 Rada Európy (1981), Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, ETS č. 108, 1981.

791 Rada Európy (2001), Dodatkový protokol k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov týkajúci sa orgánov dozoru a cezhraničných tokov údajov, ETS č. 108.

792 Rada Európy, Výbor ministrov (1987), Odporúčanie členským štátom Rec (87)15, ktorým sa upravuje používanie osobných údajov v policajnom sektore, (prijaté Výborom ministrov 17. septembra 1987 na 410. zasadnutí zástupcov ministrov).

Smernica EÚ o záznamoch o cestujúcich

Pri údajoch zo záznamu o cestujúcom (PNR) ide o informácie o cestujúcich v leteckej doprave, ktoré leteckí dopravcovia získavajú a uchovávajú v rezervačných a odletových kontrolných systémoch pri odlete na ich vlastné komerčné účely. Tieto údaje obsahujú niekoľko rôznych druhov informácií, napríklad dátumy cesty, trasu cesty, informácie o letenke, kontaktné údaje, cestovnú agentúru, u ktorej sa let objednával, použitý spôsob platby, číslo sedadla a informácie o batožine⁷⁹³. Spracúvanie údajov PNR orgánom presadzovania práva môže pomôcť pri identifikácii známych alebo potenciálnych podozrivých osôb a posúdení cestovných zvyklostí a iných ukazovateľov, ktoré sa zvyčajne spájajú s trestnou činnosťou. Analýza údajov PNR umožňuje aj spätné sledovanie cestovných trás a kontaktov osôb podozrivých z účasti na trestnej činnosti, čo orgánom presadzovania práva umožňuje identifikovať zločinecké siete⁷⁹⁴. Ako sa vysvetľuje v **oddiele 7**, EÚ uzavrela s tretími krajinami určité dohody o výmene údajov PNR. Okrem toho zaviedla spracúvanie údajov PNR v rámci EÚ prostredníctvom smernice (EÚ) 2016/681 o využívaní údajov zo záznamov o cestujúcich na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti (smernica EÚ o PNR)⁷⁹⁵. V tejto smernici sa stanovujú povinnosti leteckých dopravcov prenášať údaje PNR príslušným orgánom a zavádzajú sa prísne záruky ochrany údajov pri spracúvaní a získavaní takýchto údajov. Smernica EÚ o záznamoch o cestujúcich sa vzťahuje na medzinárodné lety do EÚ a z EÚ, ale aj na lety v rámci EÚ, ak o tom rozhodne členský štát⁷⁹⁶.

Získané údaje PNR môžu obsahovať len informácie, ktoré sú povolené podľa smernice EÚ o PNR. Musia sa uchovávať v jedinom útvere informácií na bezpečnom mieste v každom členskom štáte. Údaje PNR sa musia depersonalizovať po uplynutí šiestich mesiacov od ich poskytnutia od leteckého dopravcu a uchovávať maximálne päť rokov⁷⁹⁷. Údaje PNR sa vymieňajú medzi členskými štátmi; medzi členskými štátmi a Europolom; a s tretími krajinami, ale len v jednotlivých prípadoch.

793 Európska komisia (2011), Návrh smernice Európskeho parlamentu a Rady o využívaní údajov z osobných záznamov o cestujúcich na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti, KOM(2011) 32 v konečnom znení, Brusel, 2. februára 2011, s. 1.

794 Európska komisia (2015), Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, Brusel, 11. januára 2015.

795 Smernica Európskeho parlamentu a Rady (EÚ) 2016/681 z 27. apríla 2016 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti, Ú. v. EÚ L 119, 2016, s. 132.

796 Smernica o záznamoch o cestujúcich, Ú. v. EÚ L 119, 2016, s. 132, článok 1 ods. 1 a článok 2 ods. 1.

797 Tamže, článok 12 ods. 1 a 2.

Poskytnutie a spracúvanie údajov PNR a zaručené práva dotknutých osôb musia byť v súlade so smernicou o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní a musia zabezpečovať vysokú úroveň ochrany súkromia a osobných údajov, ktorá sa vyžaduje v Charte, modernizovanom Dohovore č. 108 a ECHR.

Nezávislé národné dozorné orgány príslušné podľa smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní sú zodpovedné aj za poradenstvo a monitorovanie uplatňovania ustanovení prijatých členskými štátmi podľa smernice EÚ o PNR.

Uchovávanie telekomunikačných údajov

Smernicou o uchovávaní údajov⁷⁹⁸ – vyhlásená za neplatnú 8. apríla 2014 v rozsudku vo veci *Digital Rights Ireland* – sa ukladala poskytovateľom komunikačných služieb povinnosť uchovávať metaúdaje dostupné na konkrétny účel boja proti závažnej trestnej činnosti počas aspoň šiestich, ale nie viac ako 24 mesiacov, bez ohľadu na to, či tieto údaje poskytovateľ stále potrebuje na účely fakturácie alebo z technického hľadiska na poskytovanie služby.

Uchovávanie telekomunikačných údajov jednoznačne zasahuje do práva na ochranu údajov⁷⁹⁹. Odôvodnenosť tohto zásahu bola napadnutá vo viacerých súdnych konaniach v členských štátoch EÚ⁸⁰⁰.

Príklad: Vo veciach *Digital Rights Ireland* a *Kärntner Landesregierung a i.*⁸⁰¹ skupina Digital Rights podala žalobu na High Court v Írsku a pán Seitlinger podal žalobu na Ústavný súd v Rakúsku, v ktorých napadli zákonnosť vnútroštátnych opatrení umožňujúcich uchovávanie údajov z elektronických komunikácií. Digital Rights požiadala írsky súd o vyhlásenie neplatnosti

798 Smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES, Ú. v. EÚ L 105, 2006.

799 EDPS (2011), *Stanovisko Európskeho dozorného úradníka pre ochranu údajov k hodnotiacej správe Komisie Rade a Európskemu parlamentu o smernici o uchovávaní údajov (smernica 2006/24/ES)*, 31. mája 2011.

800 Nemecko, Spolkový ústavný súd (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. marca 2010; Rumunsko, Federálny ústavný súd (*Curtea Constituțională a României*), č. 1258, 8. októbra 2009; Česká republika, Ústavný súd (Ústavní soud České republiky), 94/2011 Zb., 22. marca 2011.

801 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014, bod 65.

smernice 2006/24 a časti vnútroštátneho trestného zákona týkajúceho sa teroristických trestných činov. Podobne pán Seitlinger a viac ako 11 000 ďalších navrhovateľov napadli ustanovenie rakúskeho zákona o telekomunikáciách, ktorým sa preberá smernica 2006/24, a žiadali o jeho zrušenie.

V reakcii na tieto návrhy na začatie prejudiciálneho konania SDEÚ vyhlásil smernicu o uchovávaní údajov za neplatnú. Podľa SDEÚ údaje, ktoré by sa podľa smernice mohli uchovávať, poskytujú ako celok presné informácie o jednotlivcoch. Okrem toho SDEÚ preskúmal závažnosť zásahu do základných práv na rešpektovanie súkromného života a ochranu osobných údajov. Konštatoval, že uchovávanie sleduje cieľ verejného záujmu, a to boj proti závažnej trestnej činnosti, a teda cieľ v oblasti verejnej bezpečnosti. SDEÚ však uviedol, že zákonodarca EÚ prijatím smernice porušil zásadu proporcionality. Hoci smernica môže byť vhodná na dosiahnutie požadovaného cieľa, „obsahuje zásah do týchto základných práv, ktorý rozsiahlo a mimoriadne závažne zasahuje do právneho poriadku Únie bez toho, aby bol presne vymedzený ustanoveniami, ktoré by mohli zaručiť, že sa tento zásah obmedzí iba na to najnevyhnutnejšie“.

Pokiaľ neexistujú osobitné právne predpisy o uchovávaní údajov, uchovávanie údajov je prípustné ako výnimka z dôvernosti telekomunikačných údajov podľa smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách) ako preventívne opatrenie, ale len na účely boja proti závažnej trestnej činnosti⁸⁰². Takéto uchovávanie sa musí obmedziť na to, čo je nevyhnutne potrebné, pokiaľ ide o kategórie uchovávaných údajov, dotknuté komunikačné prostriedky, dotknuté osoby a zvolenú dobu uchovávania. Vnútroštátne orgány môžu mať prístup k uchovávaným údajom za prísnych podmienok vrátane predchádzajúceho preskúmania nezávislým orgánom. Údaje sa musia uchovávať v rámci EÚ.

Príklad: V nadväznosti na rozsudok vo veciach *Digital Rights Ireland* a *Kärntner Landesregierung* a i.⁸⁰³ boli SDEÚ predložené ďalšie dve veci týkajúce sa všeobecnej povinnosti uchovávať telekomunikačné údaje podľa zrušenej smernice o uchovávaní údajov, ktorá bola poskytovateľom elektronických

802 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 2002.

803 SDEÚ, spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources* a i. a *Kärntner Landesregierung* a i. [VK], 8. apríla 2014.

komunikačných služieb uložená vo Švédsku a v Spojenom kráľovstve. Vo veciach *Tele2 Sverige a Home Department/Tom Watson a i.*⁸⁰⁴ SDEÚ rozhodol, že vnútroštátne právne predpisy, ktoré predpisujú všeobecné a nediferencované uchovávanie údajov bez toho, aby vyžadovali akúkoľvek súvislosť medzi údajmi, ktoré sa musia uchovávať, a hrozbou pre verejnú bezpečnosť, a bez spresnenia akýchkoľvek podmienok – napr. obdobie uchovávania, zemepisná oblasť, okruh osôb, ktoré môžu byť zapojené do závažnej trestnej činnosti – presahujú rámec toho, čo je prísne nevyhnutné, a nemožno ich považovať za odôvodnené v demokratickej spoločnosti, ako sa vyžaduje v smernici 2002/58/ES vykladanej v spojení s Chartou základných práv EÚ.

Výhľad

V januári 2017 Európska komisia uverejnila návrh nariadenia o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách, ktorým sa mala zrušiť a nahradiť smernica 2002/58/ES⁸⁰⁵. Návrh neobsahuje žiadne osobitné ustanovenia o uchovávaní údajov. Stanovuje však, že členské štáty môžu obmedziť určité povinnosti a práva na základe právnych predpisov, ak takéto obmedzenie predstavuje potrebné a primerané opatrenie na ochranu konkrétnych verejných záujmov, ku ktorým patrí národná bezpečnosť, obrana, verejná bezpečnosť, predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, ako aj výkon trestných sankcií⁸⁰⁶. S ohľadom na judikatúru SDEÚ týkajúcu sa výkladu smernice o súkromí a elektronických komunikáciách a Charty základných práv si preto členské štáty môžu slobodne ponechať alebo vytvoriť národné rámce pre uchovávanie údajov, v rámci ktorých okrem iného stanovujú opatrenia pre cieľené uchovávanie údajov, a to pod podmienkou, že tieto rámce sú v súlade so všeobecnými zásadami práva Únie⁸⁰⁷. V čase prípravy príručky prebiehali rokovania o prijatí tohto nariadenia.

804 SDEÚ, spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.* [VK], 21. decembra 2016.

805 Európska komisia (2017), *návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (nariadenie o súkromí a elektronických komunikáciách)*, COM(2017) 10 final, Brusel, 10. januára 2017.

806 Tamže, odôvodnenie 26.

807 Pozri dôvodovú správu k návrhu nariadenia o súkromí a elektronických komunikáciách, COM (2017) 10 final, bod 1.3.

Zastrešujúca dohoda medzi EÚ a USA o ochrane osobných údajov vymieňaných na účely presadzovania práva

Zastrešujúca dohoda medzi EÚ a USA o spracúvaní osobných údajov na účely prevencie, vyšetrovania, odhaľovania a stíhania trestných činov nadobudla platnosť 1. februára 2017⁸⁰⁸. Zastrešujúca dohoda medzi EÚ a USA má za cieľ zabezpečiť vysokú úroveň ochrany údajov pre občanov EÚ a zároveň posilniť spoluprácu orgánov presadzovania práva EÚ a USA. Dopĺňa existujúce dohody medzi EÚ a USA a medzi orgánmi presadzovania práva členských štátov a USA a zároveň pomáha pri zavádzaní jasných a harmonizovaných pravidiel ochrany údajov pre budúce dohody v tejto oblasti. V tejto súvislosti je cieľom dohody vytvoriť trvalý právny rámec na uľahčenie výmeny informácií.

Dohoda sama osebe neposkytuje vhodný právny základ na výmenu osobných údajov, ale namiesto toho poskytuje dotknutým jednotlivcom vhodné záruky ochrany údajov. Vztahuje sa na každé spracúvanie osobných údajov potrebné na predchádzanie trestným činom vrátane terorizmu, ich vyšetrovanie, odhaľovanie a stíhanie⁸⁰⁹.

V dohode sa stanovujú viaceré záruky s cieľom zabezpečiť, aby sa osobné údaje používali len na účely uvedené v dohode. Občanom EÚ poskytuje najmä túto ochranu:

- obmedzenie použitia údajov: osobné údaje sa môžu použiť len na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania,
- ochrana proti svojvoľnej a neopodstatnenej diskriminácii,
- následné prenosy: každý ďalší prenos do krajiny mimo USA, mimo EÚ alebo do medzinárodnej organizácie musí podliehať predchádzajúcemu súhlasu príslušného orgánu krajiny, ktorý tieto údaje pôvodne poskytol,

808 Pozri Rada EÚ (2016), „Posilnené práva na ochranu údajov pre občanov EÚ v oblasti spolupráce na účely presadzovania práva: EÚ a Spojené štáty podpisujú zastrešujúcu dohodu“, tlačová správa 305/16, 2. júna 2016.

809 Dohoda medzi Spojenými štátmi americkými a Európskou úniou o ochrane osobných informácií v súvislosti s predchádzaním trestným činom, ich vyšetrovaním, odhaľovaním a stíhaním z 18. mája 2016, (OR.en) 8557/16, článok 3 ods. 1. Pozri aj oznámenie Komisie o rokovaniach o dohode o ochrane údajov medzi EÚ a USA z 26. mája 2010, (MEMO/10/216) a tlačovú správu Komisie (2010) o vysokej úrovni ochrany súkromia v dohode medzi EÚ a USA o ochrane údajov z 26. mája 2010, IP/10/609.

- kvalita údajov: osobné údaje sa musia uchovávať vzhľadom na ich správnosť, relevantnosť, aktuálnosť a úplnosť,
- bezpečnosť spracúvania vrátane oznamovania porušení ochrany osobných údajov,
- spracúvanie citlivých údajov je povolené len vtedy, ak existujú primerané záruky v súlade s právnym predpisom,
- doby uchovávania: osobné údaje nesmú byť uchovávané dlhšie, ako je nevyhnutné alebo primerané,
- práva na prístup a opravu: každý jednotlivec má právo na prístup k svojim osobným údajom za určitých podmienok a bude môcť požiadať o opravu nesprávnych údajov,
- automatizované rozhodnutia si vyžadujú primerané záruky vrátane možnosti dosiahnuť ľudský zásah,
- účinný dozor vrátane spolupráce medzi dozornými orgánmi EÚ a USA a
- súdne prostriedky nápravy a vykonateľnosť: občania EÚ majú právo⁸¹⁰ domáhať sa súdnych prostriedkov nápravy na súdoch Spojených štátov v prípadoch, keď im americké orgány odmietnu prístup k ich osobným údajom alebo ich opravu, alebo tieto osobné údaje protiprávne zverejnia.

V rámci „zastrešujúcej dohody“ bol zriadený aj systém, v rámci ktorého sa v prípade potreby informuje príslušný dozorný orgán v členskom štáte dotknutých fyzických osôb o akomkoľvek porušení ochrany údajov. Právne záruky, ktoré dohoda poskytuje, zabezpečujú v prípade porušenia súkromia rovnaké zaobchádzanie s občanmi EÚ v USA⁸¹¹.

810 Zákon o súdnych prostriedkoch nápravy podpísal prezident Obama 24. februára 2016.

811 Európsky dozorný úradník pre ochranu údajov vydal stanovisko k dohode medzi EÚ a USA, v ktorom odporúča okrem iného tieto úpravy: 1. doplniť „na osobitné účely, na ktoré boli prenesené“ do článku, ktorý sa týka neuchovávaní údajov na obdobie dlhšie, ako je nevyhnutné a primerané, a 2. vylúčiť možné hromadné prenosy citlivých údajov. Pozri Európsky dozorný úradník pre ochranu údajov, [Stanovisko 1/2016 Predbežné stanovisko k dohode medzi Spojenými štátmi americkými a Európskou úniou o ochrane osobných informácií v súvislosti s prevenciou, vyšetrovaním, zisťovaním a stíhaním trestných činov](#), bod 35.

8.3.1. Ochrana údajov v súdnych orgánoch a orgánoch presadzovania práva EÚ

Europol

Agentúra EÚ na presadzovanie práva – Europol – sídli v Haagu a v každom členskom štáte má národnú ústredňu. Europol bol zriadený v roku 1998 a jeho súčasné právne postavenie ako inštitúcie EÚ je založené na nariadení o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (nariadenie o Europole)⁸¹². Cieľom Europolu je pomáhať pri prevencii a vyšetrowaní organizovanej trestnej činnosti, terorizmu a ďalších foriem závažnej trestnej činnosti (ako sú uvedené v prílohe I nariadenia o Europole), ktoré sa týkajú dvoch alebo viacerých členských štátov. Tento cieľ dosahuje prostredníctvom výmeny informácií a činnosťou informačného centra EÚ, ktoré poskytuje spravodajské analýzy a hodnotenia hrozieb.

Europol zriadil v záujme dosiahnutia svojich cieľov Informačný systém Europolu, ktorý poskytuje členským štátom databázu na výmenu spravodajských informácií o trestnej činnosti a výmenu informácií prostredníctvom národných ústrední. Informačný systém Europolu sa môže použiť na sprístupnenie údajov, ktoré sa týkajú: osôb podozrivých alebo obvinených zo spáchania trestného činu patriaceho do rozsahu pôsobnosti Europolu alebo osôb, pri ktorých existujú konkrétne náznaky, že takéto trestné činy spáchajú. Europol a národné ústredne môžu zadávať údaje priamo do Informačného systému Europolu a získavať z neho informácie. Údaje zadané do systému smie upravovať, opravovať alebo vymazávať len strana, ktorá ich zadala. Informácie môžu Europolu poskytovať aj orgány EÚ, tretie krajiny a medzinárodné organizácie.

Informácie vrátane osobných údajov môže Europol získať aj z verejne dostupných zdrojov, ako je internet. Prenosy osobných údajov orgánom EÚ sú povolené len vtedy, ak je to potrebné na plnenie úlohy Europolu alebo prijímajúceho orgánu EÚ. Prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám sú povolené len vtedy, ak Európska komisia rozhodne, že daná krajina alebo medzinárodná organizácia zabezpečuje primeranú úroveň ochrany údajov („rozhodnutie o primeranosti“), alebo ak existuje medzinárodná dohoda alebo dohoda o spolupráci. Europol môže prijímať a spracúvať osobné údaje od súkromných subjektov

812 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol), ktorým sa nahrádzajú a zrušujú rozhodnutia Rady 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, Ú. v. EÚ L 135, 2016, s. 53.

a súkromných osôb za prísnych podmienok, že tieto údaje zasiela národná ústredňa Europolu v súlade s vnútroštátnym právom, kontaktné miesto v tretej krajine alebo medzinárodná organizácia, s ktorou existuje spolupráca prostredníctvom dohody o spolupráci, alebo orgán tretej krajiny alebo medzinárodná organizácia, na ktorú sa vzťahuje rozhodnutie o primeranosti alebo s ktorou EÚ uzavrela medzinárodnú dohodu. Všetky výmeny informácií sa uskutočňujú prostredníctvom sieťovej aplikácie na zabezpečenú výmenu informácií (SIENA).

V reakcii na nový vývoj sa v rámci Europolu zriadili špecializované centrá. V roku 2013 bolo v rámci Europolu zriadené Európske centrum boja proti počítačovej kriminalite⁸¹³. Centrum slúži ako informačné stredisko EÚ v oblasti počítačovej kriminality, pomáha zrýchliť odozvu na trestnú činnosť on-line, vyvíja a zavádza digitálne forenzné funkcie a poskytuje najlepšie praktické postupy pri vyšetrovaní počítačovej kriminality. Centrum sa zameriava na počítačovú kriminalitu:

- páchanú organizovanými skupinami s cieľom nadobudnúť veľké zisky z trestnej činnosti, napríklad internetové podvody,
- spôsobujúcu vážne poškodenie obetí, napríklad sexuálne vykorisťovanie detí on-line,
- ovplyvňujúcu kritickú infraštruktúru a informačné systémy v EÚ.

Európske centrum pre boj proti terorizmu (ECTC) bolo vytvorené v januári 2016 s cieľom poskytnúť členským štátom operačnú podporu pri vyšetrovaniach týkajúcich sa teroristických trestných činov. V reálnom čase porovnáva operačné údaje s údajmi, ktoré Europol už má k dispozícii, čo vedie k rýchlemu získaniu finančných stôp, a analyzuje všetky dostupné údaje z vyšetrovaní s cieľom pomôcť pri zostavovaní štruktúrovaného obrazu o teroristickej sieti⁸¹⁴.

Európske stredisko pre boj proti prevádzacstvu (EMSC) bolo zriadené vo februári 2016 v nadväznosti na zasadnutie Rady v novembri 2015 s cieľom podporiť členské štáty pri zameriavaní sa na zločinecké siete zapojené do prevádzacstva migrantov a ich rozkladaní. Pôsobí ako informačné centrum na podporu osobitnej regionálnej jednotky EÚ v mestách Catania (Taliansko) a Piraeus (Grécko), ktoré pomáhajú

813 Pozri tiež EDPS (2012), *Stanovisko Európskeho dozorného úradníka pre ochranu údajov k oznámeniu Európskej komisie Rade a Európskemu parlamentu o zriadení Európskeho centra boja proti počítačovej kriminalite*, Brusel, 29. júna 2012.

814 Pozri [webovú stránku Europolu o ECTC](#).

vnútroštátnym orgánom vo viacerých oblastiach vrátane výmeny spravodajských informácií, vyšetrovania trestných činov a stíhania zločineckých sietí prevádzkačov⁸¹⁵.

Činnosti Europolu sa riadia posilneným režimom ochrany údajov, ktorý vychádza zo zásad nariadenia o ochrane údajov inštitúciami EÚ⁸¹⁶ a je tiež v súlade so smernicou o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, modernizovaným Dohovorom č. 108 a odporúčaním v oblasti polície.

Spracúvanie osobných údajov týkajúcich sa obetí trestných činov, svedkov alebo iných osôb, ktoré môžu poskytnúť informácie o trestných činoch, alebo týkajúcich sa osôb mladších ako 18 rokov je povolené, pokiaľ to je bezpodmienečne nevyhnutné a primerané na účely predchádzania trestnej činnosti alebo boja proti nej v rámci cieľov Europolu⁸¹⁷. Spracúvanie citlivých osobných údajov je zakázané, pokiaľ to nie je bezpodmienečne nevyhnutné a primerané na účely predchádzania trestnej činnosti alebo boja proti nej v rámci cieľov Europolu a pokiaľ tieto údaje nedoplňajú iné osobné údaje, ktoré Europol spracúval⁸¹⁸. V oboch týchto prípadoch má prístup k relevantným údajom len Europol⁸¹⁹.

Uchovávanie údajov je povolené len na nevyhnutný a primeraný čas a jeho pokračovanie podlieha každé tri roky preskúmaniu, bez ktorého sa údaje automaticky vymažú⁸²⁰.

Europol môže za určitých podmienok priamo prenášať osobné údaje orgánu EÚ alebo orgánu tretej krajiny, alebo medzinárodnej organizácii⁸²¹. Porušenia ochrany údajov, ak by mali pravdepodobne závažný a nepriaznivý vplyv na práva a slobody dotknutých osôb, sa dotknutým osobám musia bez zbytočného odkladu oznámiť⁸²². Na úrovni členských štátov bude vymenovaný národný dozorný orgán, ktorý bude monitorovať spracúvanie osobných údajov Europolom⁸²³.

815 Pozri [webovú stránku Europolu o EMSC](#).

816 Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov, Ú. v. ES L 8, 2001.

817 Nariadenie o Europole, článok 30 ods. 1.

818 Tamže, článok 30 ods. 2.

819 Tamže, článok 30 ods. 3.

820 Tamže, článok 31.

821 Tamže, články 24 a 25.

822 Tamže, článok 35.

823 Nariadenie o Europole, článok 42.

EDPS je zodpovedný za monitorovanie a zabezpečenie ochrany základných práv a slobôd fyzických osôb, pokiaľ ide o spracúvanie osobných údajov Europolom, a za poskytovanie poradenstva Europolu a dotknutým osobám vo všetkých otázkach týkajúcich sa spracúvania osobných údajov. EDPS preto koná ako orgán na vyšetrovanie a vybavovanie sťažností a úzko spolupracuje s národnými dozornými orgánmi⁸²⁴. EDPS a národné dozorné orgány sa budú stretávať aspoň dvakrát ročne v rámci Rady pre spoluprácu, ktorá má poradnú funkciu⁸²⁵. Členské štáty sú na základe právnych predpisov povinné zriadiť dozorný orgán, ktorý bude príslušný na monitorovanie prípustnosti prenosu osobných údajov z úrovne členského štátu Europolu, ako aj prípustnosti vyhľadávania osobných údajov a ich oznamovania Europolu⁸²⁶. Od členských štátov sa takisto vyžaduje, aby zabezpečili, že národný dozorný orgán môže pri plnení svojich úloh a povinností vyplývajúcich z nariadenia o Europole konať úplne nezávisle⁸²⁷. Europol uchováva protokoly alebo dokumentáciu svojich činností spracúvania údajov na účely overenia zákonnosti spracúvania osobných údajov, na vlastné monitorovanie a na zaistenie riadnej integrity a bezpečnosti údajov. Tieto protokoly obsahujú informácie o spracovateľských operáciách v systémoch automatizovaného spracúvania, ktoré sa týkajú získavania, zmeny, nahliadnutia, prístupnosti, kombinovania a vymazania⁸²⁸.

Odvolať sa proti rozhodnutiu EDPS možno podať na SDEÚ⁸²⁹. Každá osoba, ktorá utrpela škodu v dôsledku nezákonnej operácie spracúvania, má právo na náhradu spôsobenej škody buď od Europolu, alebo od zodpovedného členského štátu, a to podaním žaloby na SDEÚ v prvom prípade alebo na príslušný vnútroštátny súd v druhom prípade⁸³⁰. Okrem toho môže činnosť Europolu kontrolovať špecializovaná spoločná parlamentná kontrolná skupina národných parlamentov a Európskeho parlamentu⁸³¹. Každá osoba má právo na prístup k akýmkoľvek osobným údajom, ktoré by o nej Europol mohol uchovávať, ako aj právo požiadať o kontrolu, opravu alebo vymazanie týchto údajov. Na tieto práva sa môžu vzťahovať výnimky a obmedzenia.

824 Tamže, články 43 a 44.

825 Tamže, článok 45.

826 Tamže, článok 42 ods. 1.

827 Tamže, článok 42 ods. 1.

828 Tamže, článok 40.

829 Tamže, článok 48.

830 Tamže, článok 50.

831 Tamže, článok 51.

Eurojust

Eurojust, zriadený v roku 2002, je orgán EÚ so sídlom v Haagu. Podporuje justičnú spoluprácu pri vyšetrovaní a stíhaní závažnej trestnej činnosti týkajúcej sa minimálne dvoch členských štátov⁸³². Eurojust je oprávnený:

- podporovať a zlepšovať koordináciu vyšetrovaní a stíhaní medzi príslušnými orgánmi rôznych členských štátov,
- podporovať vykonávanie žiadostí a rozhodnutí týkajúcich sa súdnej spolupráce.

Funkcie Eurojustu vykonávajú národní členovia. Každý členský štát vysielá do Eurojustu jedného sudcu alebo prokurátora, ktorého postavenie je upravené vnútroštátnymi právnymi predpismi a ktorý má právomoci nevyhnutne potrebné na plnenie úloh nutných na podporu a zlepšovanie justičnej spolupráce. Jednotliví národní členovia Eurojustu okrem toho konajú spoločne ako kolégium pri plnení osobitných úloh Eurojustu.

Eurojust môže spracúvať osobné údaje do tej miery, do akej je to nutné na dosiahnutie jeho cieľov. Spracúvanie údajov je však obmedzené na konkrétne informácie týkajúce sa osôb, ktoré sú podozrivé zo spáchania trestného činu alebo účasti na ňom, alebo boli odsúdené za spáchanie trestného činu v rozsahu právomoci Eurojustu. Eurojust môže tiež spracúvať určité informácie týkajúce sa svedkov alebo obetí trestných činov v rozsahu svojej pôsobnosti⁸³³. Za výnimočných okolností Eurojust môže na určité obmedzené obdobie spracúvať rozsiahlejšie osobné údaje týkajúce sa okolností trestného činu, ak sa tieto údaje bezprostredne týkajú prebiehajúceho vyšetrovania. Eurojust môže v rozsahu svojej pôsobnosti spolupracovať s ostatnými inštitúciami, orgánmi a agentúrami EÚ a vymieňať si s nimi osobné údaje. Eurojust môže tiež spolupracovať a vymieňať si osobné údaje s tretími krajinami a organizáciami.

832 Rada Európskej únie (2002), rozhodnutie Rady 2002/187/SVV z 28. februára 2002, ktorým sa zriaďuje Eurojust s cieľom posilniť boj proti závažným trestným činom, Ú. v. ES L 63, 2002; Rada Európskej únie (2003), rozhodnutie Rady 2003/659/SVV z 18. júna 2003, ktorým sa mení a dopĺňa rozhodnutie 2002/187/SVV, ktorým sa zriaďuje Eurojust s cieľom posilniť boj proti závažným trestným činom, Ú. v. EÚ L 245, 2003; Rada Európskej únie (2009), rozhodnutie Rady 2009/426/SVV zo 16. decembra 2008 o posilnení Eurojustu a o zmene a doplnení rozhodnutia Rady 2002/187/SVV, ktorým sa zriaďuje Eurojust s cieľom posilniť boj proti závažným trestným činom, Ú. v. EÚ L 138, 2009 (rozhodnutia o Eurojuste).

833 Konsolidované znenie rozhodnutia Rady z 28. februára 2002, zmeneného rozhodnutím Rady 2003/659/SVV a rozhodnutím Rady 2009/426/SVV, článok 15 ods. 2.

Pokiaľ ide o ochranu údajov, Eurojust musí zaručiť úroveň ochrany aspoň rovnocennú so zásadami podľa modernizovaného Dohovoru Rady Európy č. 108 v znení následných zmien. V prípadoch výmeny údajov musí dodržiavať osobitné pravidlá a obmedzenia, ktoré sú stanovené buď v dohode o spolupráci, alebo pracovných podmienkach v súlade s rozhodnutiami Rady o Eurojuste a pravidlami ochrany údajov v Eurojuste⁸³⁴.

V rámci Eurojustu funguje nezávislý spoločný dozorný orgán poverený monitorovaním spracúvania osobných údajov zo strany Eurojustu. Ak jednotlivci nie sú spokojní s odpoveďou Eurojustu na žiadosť o prístup k osobným údajom, ich úpravu, zablokovanie alebo vymazanie, môžu sa odvolať na spoločný dozorný orgán. Ak Eurojust spracúva osobné údaje nezákonne, je v súlade s právnymi predpismi toho členského štátu, v ktorom má sídlo, teda Holandska, zodpovedný za všetky škody spôsobené dotknutým osobám.

Výhľad

Európska komisia predložila v júli 2013 návrh nariadenia o reforme Eurojustu. K tomuto návrhu bol pripojený návrh na zriadenie Európskej prokuratúry (pozri nižšie). Cieľom tohto nariadenia je zosúladiť funkcie a štruktúru Eurojustu s Lisabonskou zmluvou. Cieľom reformy je okrem toho jasne vymedziť operačné úlohy Eurojustu, ktoré vykonáva kolégium Eurojustu, a jeho administratívne úlohy. Umožní sa tým aj to, aby sa členské štáty viac zameriavali na operačné úlohy. Zriadi sa nová výkonná rada, ktorá bude pomáhať kolégiu pri plnení administratívnych úloh⁸³⁵.

Európska prokuratúra

Členské štáty majú výlučnú právomoc stíhať trestné činy podvodov a nenáležité plnenia rozpočtu EÚ, ktoré majú aj potenciálne cezhraničné dôsledky. Význam vyšetrovania, stíhania a odsúdenia páchateľov takýchto trestných činov narastá, a to najmä vzhľadom na prebiehajúcu hospodársku krízu⁸³⁶. Európska komisia navrhla nariadenie o zriadení nezávislej Európskej prokuratúry (EPPO)⁸³⁷ s cieľom bojovať

834 Ustanovenia vnútorných predpisov Eurojustu týkajúce sa spracovania a ochrany osobných údajov, Ú. v. EÚ C 68, 19. marca 2005, s. 1.

835 Pozri [webovú stránku Európskej komisie o Eurojuste](#).

836 Pozri Európska komisia (2013), návrh nariadenia Rady o zriadení Európskej prokuratúry, COM(2013) 534 final, Brusel, 17. júla 2013, s. 1 a [webovú stránku Komisie o Európskej prokuratúre](#).

837 Európska komisia (2013), návrh nariadenia Rady o zriadení Európskej prokuratúry, COM(2013) 534 final, Brusel, 17. júla 2013.

proti trestným činom poškodzujúcim finančné záujmy EÚ. Európska prokuratúra sa zriadi na základe postupu posilnenej spolupráce, ktorý umožňuje minimálne deviatim členským štátom nadviazať posilnenú spoluprácu v oblasti v rámci štruktúr EÚ bez zapojenia ostatných krajín EÚ⁸³⁸. Belgicko, Bulharsko, Cyprus, Česká republika, Estónsko, Fínsko, Francúzsko, Grécko, Chorvátsko, Litva, Lotyšsko, Luxembursko, Nemecko, Portugalsko, Rumunsko, Slovensko, Slovinsko a Španielsko sa pripojili k posilnenej spolupráci; Rakúsko a Taliansko vyjadrili úmysel pripojiť sa⁸³⁹.

Európska prokuratúra bude oprávnená vyšetrovať a stíhať podvody EÚ a iné trestné činy poškodzujúce finančné záujmy EÚ s cieľom účinne koordinovať vyšetrovanie a stíhanie v rámci rôznych vnútroštátnych právnych poriadkov a zlepšiť využívanie zdrojov a výmenu informácií na európskej úrovni⁸⁴⁰.

Európsku prokuratúru povedie európsky prokurátor, pričom v každom členskom štáte bude pôsobiť aspoň jeden delegovaný európsky prokurátor, ktorý má na starosti vyšetrovanie a trestné stíhanie v danom členskom štáte.

V návrhu sa stanovujú prísne záruky na zaručenie práv osôb zapojených do vyšetrovania Európskej prokuratúry, ako sú stanovené vo vnútroštátnom práve, v práve EÚ a v Charte základných práv Európskej únie. Vyšetrovacie opatrenia, ktoré sa dotýkajú najmä základných práv, si budú vyžadovať predchádzajúce schválenie vnútroštátneho súdu⁸⁴¹. Vyšetrovania Európskej prokuratúry podliehajú súdnemu preskúmaniu zo strany vnútroštátnych súdov⁸⁴².

Na spracúvanie administratívnych osobných údajov, ktoré vykonáva Európska prokuratúra, sa bude vzťahovať nariadenie o ochrane údajov inštitúciami EÚ⁸⁴³. Pokiaľ ide o spracúvanie osobných údajov týkajúcich sa operačných záležitostí, Európska prokuratúra bude, podobne ako Europol, uplatňovať samostatný režim ochrany

838 Zmluva o fungovaní EÚ, článok 86 ods. 1 a článok 329 ods. 1.

839 Pozri Rada Európskej únie (2017), „*20 členských štátov sa dohodlo na podrobnostiach o vytvorení Európskej prokuratúry*“, tlačová správa, 8. júna 2017.

840 Európska komisia (2013), návrh nariadenia Rady o zriadení Európskej prokuratúry, COM(2013) 534 final, Brusel, 17. júla 2013 s. 1 a s. 51 – 51. Pozri tiež *webovú stránku Európskej komisie o Európskej prokuratúre*.

841 Európska komisia (2013), návrh nariadenia Rady o zriadení Európskej prokuratúry, COM(2013) 534 final, Brusel, 17. júla 2013, článok 26 ods. 4.

842 Tamže, článok 36.

843 Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov, Ú. v. ES L 8, 2001.

údajov podobný systému, ktorým sa riadia činnosti Europolu a Eurojustu, vzhľadom na to, že vykonávanie funkcií Európskej prokuratúry bude zahŕňať spracúvanie osobných údajov orgánmi presadzovania práva a trestného stíhania na úrovni členských štátov. Pravidlá ochrany údajov Európskej prokuratúry sú preto takmer rovnaké ako pravidlá podľa smernice o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní. Podľa návrhu na zriadenie Európskej prokuratúry spracúvanie osobných údajov musí byť v súlade so zásadami zákonnosti a spravodlivosti, obmedzenia účelu, minimalizácie údajov, presnosti, integrity a dôvernosti. Európska prokuratúra musí v čo najväčšej miere jasne rozlišovať medzi osobnými údajmi rôznych druhov dotknutých osôb, ako sú osoby odsúdené za trestný čin, osoby, ktoré sú len podozrivými, obeťami a svedkami. Takisto sa musí snažiť overiť kvalitu spracúvaných osobných údajov a v čo najväčšej miere rozlišovať medzi osobnými údajmi založenými na faktoch a osobnými údajmi založenými na osobných hodnoteniach.

Návrh obsahuje ustanovenia o právach dotknutých osôb, najmä o právach na informácie, prístup k osobným údajom, opravu, vymazanie a obmedzenie spracúvania, a stanovuje sa v ňom, že takéto práva sa môžu vykonávať aj nepriamo prostredníctvom EDPS. Obsahuje takisto zásady bezpečnosti spracúvania a zodpovednosti, podľa ktorých sa vyžaduje, aby Európska prokuratúra prijala primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú rizikám, ktoré predstavuje spracúvanie, viesť záznamy o všetkých spracovateľských činnostiach a vykonať posúdenie vplyvu na ochranu údajov pred spracúvaním, ak je pravdepodobné, že druh spracúvania (napríklad spracúvanie zahŕňajúce používanie nových technológií) pravdepodobne povedie k vysokému riziku pre práva jednotlivcov. Napokon sa v návrhu stanovuje, že kolégium určí zodpovednú osobu, ktorá sa riadne zapojí do všetkých záležitostí týkajúcich sa ochrany osobných údajov a musí zabezpečiť, aby Európska prokuratúra dodržiavala príslušné právne predpisy o ochrane údajov.

8.3.2. Ochrana údajov v spoločných informačných systémoch na úrovni EÚ

Okrem výmeny údajov medzi členskými štátmi a vytvorenia špecializovaných orgánov EÚ na boj proti cezhraničnej trestnej činnosti, ako sú Europol, Eurojust a Európska prokuratúra, bolo zriadených niekoľko spoločných informačných systémov na úrovni EÚ, ktoré majú umožniť a uľahčiť spoluprácu a výmenu údajov medzi príslušnými vnútroštátnymi orgánmi a orgánmi EÚ na konkrétne účely v oblasti ochrany hraníc, prisťahovalectva a azylu a colnej správy. Keďže schengenský priestor vznikol najskôr

na základe medzinárodnej dohody, ktorá bola nezávislá od práva EÚ, Schengenský informačný systém (SIS) bol vytvorený na základe mnohostranných dohôd a až následne sa začal riadiť právnymi predpismi EÚ. Vízový informačný systém (VIS), Eurodac, EUROSUR a colný informačný systém (CIS) boli vytvorené ako nástroje, ktoré sa riadia právom EÚ.

Dohľad nad týmito systémami spoločne vykonávajú národné dozorné orgány a EDPS. Na zabezpečenie vysokej úrovne ochrany tieto orgány spolupracujú v rámci koordinačných skupín pre dohľad, ktoré sa týkajú týchto rozsiahlych informačných systémov: 1. Eurodac; 2. vízový informačný systém; 3. Schengenský informačný systém; 4. colný informačný systém a 5. informačný systém o vnútornom trhu⁸⁴⁴. Koordinačné skupiny pre dohľad sa zvyčajne stretávajú dvakrát ročne, pod vedením zvoleného predsedu, a prijímajú usmernenia, rokujú o cezhraničných prípadoch alebo prijímajú spoločné rámce pre inšpekcie.

Agentúra EÚ pre rozsiahle informačné systémy (eu-LISA)⁸⁴⁵, zriadená v roku 2012, je zodpovedná za prevádzkové riadenie Schengenského informačného systému druhej generácie (SIS II), vízového informačného systému (VIS) a systému Eurodac. Hlavnou úlohou eu-LISA je zabezpečiť účinné, bezpečné a nepretržité fungovanie systémov informačných technológií. Okrem toho je zodpovedná za prijatie potrebných opatrení na zaistenie bezpečnosti systémov a bezpečnosti údajov.

Schengenský informačný systém

V roku 1985 niekoľko členských štátov bývalého Európskeho spoločenstva podpísalo dohodu medzi Hospodárskou úniou Beneluxu, Nemeckom a Francúzskom o postupnom odstraňovaní kontrol na spoločných hraniciach (Schengenská dohoda), ktorej cieľom bolo vytvoriť oblasť voľného pohybu osôb bez pohraničnej kontroly na schengenskom území⁸⁴⁶. Ako protiváha k ohrozeniu verejnej bezpečnosti v dôsledku otvorenia hraníc boli posilnené pohraničné kontroly na vonkajších hraniciach schengenského priestoru a nadviazala sa úzka spolupráca medzi vnútroštátnymi policajnými a súdnymi orgánmi.

844 Pozri webovú stránku Európskeho dozorného úradníka pre ochranu údajov o koordinácii dohľadu.

845 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1077/2011 z 25. októbra 2011, ktorým sa zriaďuje Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti, Ú. v. EÚ L 286, 2011.

846 Dohoda medzi vládami štátov Hospodárskej únie Beneluxu, Spolkovej republiky Nemecko a Francúzskej republiky o postupnom odstraňovaní kontrol na ich spoločných hraniciach, Ú. v. ES L 239, 2000.

V dôsledku prístúpenia ďalších štátov k Schengenskej dohode bol schengenský systém napokon prostredníctvom Amsterdamskej zmluvy⁸⁴⁷ začlenený do právneho rámca EÚ. Vykonanie tohto rozhodnutia sa uskutočnilo v roku 1999. Najnovšia verzia Schengenského informačného systému, tzv. SIS II, bola uvedená do prevádzky 9. apríla 2013. V súčasnosti slúži väčšine členských štátov EÚ⁸⁴⁸ a Islandu, Lichtenštajnsku, Nórsku a Švajčiarsku⁸⁴⁹. Prístup do SIS II má aj Europol a Eurojust.

SIS II tvorí centrálny systém (C-SIS), národné systémy (N-SIS) v jednotlivých členských štátoch a komunikačná infraštruktúra medzi centrálnym systémom a národnými systémami. C-SIS obsahuje určité údaje o osobách a predmetoch zadané členskými štátmi. C-SIS používa vnútroštátna pohraničná kontrola, polícia, colníci, vízové a súdne orgány v celom schengenskom priestore. Jednotlivé členské štáty prevádzkujú kópie C-SIS, tzv. národné Schengenské informačné systémy (N-SIS), ktoré sa nepretržite aktualizujú, čím sa aktualizuje aj C-SIS. V SIS existujú rôzne druhy zápisov:

- osoba nemá právo vstúpiť na schengenské územie alebo na tomto území pobývať alebo
- po osobe alebo predmete pátrajú súdne orgány alebo orgány presadzovania práva (napr. európske zatýkacie rozkazy, žiadosti o diskretnú kontrolu), alebo
- osoba bola hlásená ako nezvestná, alebo
- tovar, napríklad bankovky, vozidlá, nákladné vozidlá, zbrane a doklady totožnosti, sú hlásené ako odcudzený alebo stratený majetok.

V prípade zápisu sa vykonávajú následné činnosti prostredníctvom útvarov SIRENE. SIS II má nové funkcie, napríklad možnosť zadania: biometrických údajov (napríklad odtlačkov prstov a fotografií) alebo nových kategórií zápisov, ktoré sa týkajú napríklad odcudzených lodí, lietadiel, kontajnerov alebo platobných prostriedkov,

847 Európske spoločenstvá (1997), Amsterdamská zmluva, ktorá mení Zmluvu o Európskej únii, zmluvy o založení Európskych spoločenstiev a niektoré súvisiace akty, Ú. v. ES C 340, 1997.

848 Chorvátsko, Cyprus a Írsko sa pripravujú na integráciu do SIS II, ale ešte nie sú jeho súčasťou. Pozri informácie o Schengenskom informačnom systéme na [webovom sídle Generálneho riaditeľstva Európskej komisie pre migráciu a vnútorné záležitosti](#).

849 Nariadenie Európskeho parlamentu a Rady (ES) č. 1987/2006 z 20. decembra 2006 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II), Ú. v. EÚ L 381, 2006 a Rada Európskej únie (2007), rozhodnutie Rady 2007/533/SVV z 12. júna 2007 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II), Ú. v. EÚ L 205, 2007.

rozšírené zápisy týkajúce sa osôb a predmetov, kópie európskych zatýkacích rozkazov pre hľadané osoby, ktoré majú nastúpiť výkon trestu odňatia slobody alebo majú byť odovzdané alebo vydané.

SIS II vychádza z dvoch aktov, ktoré sa navzájom dopĺňajú: rozhodnutie o SIS II⁸⁵⁰ a nariadenie o SIS II⁸⁵¹. Pri prijímaní tohto rozhodnutia a nariadenia zákonodarca EÚ použil rozdielne právne základy. Týmto rozhodnutím sa riadi využívanie SIS II na účely, na ktoré sa vzťahuje policajná a justičná spolupráca v trestných veciach (bývalý tretí pilier EÚ). Nariadenie sa uplatňuje na postupy zápisov v rámci vízovej, azylovej, prístahovaleckej a iných politík týkajúcich sa voľného pohybu osôb (predtým prvý pilier). Postupy zápisov pre každý pilier sa museli upraviť samostatnými aktnami vzhľadom na to, že tieto dva právne akty boli prijaté pred Lisabonskou zmluvou a pred zrušením štruktúry pilierov.

Oba právne akty obsahujú pravidlá o ochrane údajov. Rozhodnutím o SIS II sa zakazuje spracúvanie citlivých údajov⁸⁵². Na spracúvanie osobných údajov sa vzťahuje rozsah pôsobnosti modernizovaného Dohovoru č. 108⁸⁵³. Okrem toho majú osoby právo na prístup k osobným údajom, ktoré s nimi súvisia a ktoré sa zadávajú do SIS II⁸⁵⁴.

Nariadením o SIS II sa upravujú podmienky a postupy vkladania zápisov a spracúvania zápisov o odmietnutiach vstupu alebo pobytu občanov z krajín mimo EÚ. Ustanovujú sa ním aj pravidlá výmeny doplňujúcich a dodatočných informácií na účely vstupu alebo pobytu v členskom štáte⁸⁵⁵. Toto nariadenie obsahuje aj pravidlá ochrany údajov. Citlivé kategórie údajov uvedené v článku 9 ods. 1 všeobecného nariadenia o ochrane údajov sa nesmú spracúvať⁸⁵⁶. Nariadením o SIS II sa stanovujú aj určité práva dotknutej osoby, a to:

850 Rozhodnutie Rady 2007/533/SVV z 12. júna 2007 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II), Ú. v. EÚ L 205, 7.8.2007.

851 Nariadenie Európskeho parlamentu a Rady (ES) č. 1987/2006 z 20. decembra 2006 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II), Ú. v. EÚ L 381, 28.12.2006.

852 Rozhodnutie o SIS II, článok 56; nariadenie o SIS II, článok 40.

853 Rozhodnutie o SIS II, článok 57.

854 Rozhodnutie o SIS II, článok 58; nariadenie o SIS II, článok 41.

855 Nariadenie o SIS II, článok 2.

856 Tamže, článok 40.

- právo na prístup k osobným údajom súvisiacim s dotknutou osobou⁸⁵⁷,
- právo na opravu nesprávnych údajov⁸⁵⁸,
- právo na vymazanie nezákonne uložených údajov⁸⁵⁹,
- právo byť informovaný, ak existuje zápis vydaný voči dotknutej osobe. Informácie musia byť v písomnej forme a musia sa k nim priložiť kópia alebo odkaz na vnútroštátne rozhodnutie o vydaní zápisu⁸⁶⁰.

Právo byť informovaný sa neposkytne, ak 1. osobné údaje neboli získané od dotknutej osoby a za predpokladu, že poskytnutie informácií je nemožné alebo si vyžaduje vynaloženie neprimeraného úsilia; 2. dotknutá osoba už má informácie; alebo 3) ak sa podľa vnútroštátneho práva umožňuje obmedzenie na základe, okrem iného, ochrany národnej bezpečnosti alebo predchádzania trestným činom⁸⁶¹.

V prípade ako rozhodnutia o SIS II, tak aj nariadenia o SIS II sa prístupové práva jednotlivcov, pokiaľ ide o SIS II, môžu vykonávať v ktoromkoľvek členskom štáte a budú sa riešiť v súlade s vnútroštátnym právom tohto členského štátu⁸⁶².

Príklad: Vo veci *Dalea/Francúzsko*⁸⁶³ bola zamietnutá žiadosť sťažovateľa o udelenie víza na návštevu Francúzska, keďže francúzske orgány v Schengenskom informačnom systéme uviedli, že by sťažovateľovi nemal byť povolený vstup. Sťažovateľ neúspešne žiadal francúzsku Komisiu pre ochranu údajov a napokon Štátnu radu o prístup k údajom a ich úpravu alebo výmaz. ESLP dospel k záveru, že zadanie mena sťažovateľa do Schengenského informačného systému bolo v súlade s právnymi predpismi a malo legitímny cieľ ochrany národnej bezpečnosti. Keďže sťažovateľ nepreukázal, akú škodu v skutočnosti utrpel v dôsledku zamietnutia vstupu do schengenského priestoru, a keďže boli prijaté dostatočné opatrenia na ochranu sťažovateľa

857 Tamže, článok 41 ods. 1.

858 Tamže, článok 41 ods. 5.

859 Tamže, článok 41 ods. 5.

860 Tamže, článok 42 ods. 1.

861 Tamže, článok 42 ods. 2.

862 Nariadenie o SIS II, článok 41 ods. 1 a rozhodnutie o SIS, článok 58.

863 ESLP, *Dalea/Francúzsko*, č. 964/07, 2. februára 2010.

pred svojvoľnými rozhodnutiami, zásah do jeho práva na rešpektovanie súkromného života bol primeraný. Sťažnosť sťažovateľa podľa článku 8 bola teda vyhlásená za neprípustnú.

Dozor nad vnútroštátnym systémom N.SIS vykonáva príslušný vnútroštátny dozorný orgán daného členského štátu. Vnútroštátny dozorný orgán musí zabezpečiť, aby sa aspoň každé štyri roky vykonal audit operácií spracúvania údajov v rámci vnútroštátneho systému N.SIS⁸⁶⁴. Vnútroštátne dozorné orgány a EDPS spolupracujú a zabezpečujú koordinovaný dozor nad N.SIS, pričom EDPS je zodpovedný za dohľad nad systémom C.SIS. V záujme transparentnosti sa každé dva roky zašle Európskemu parlamentu, Rade a eu-LISA spoločná správa o činnosti. Koordinačná skupina pre dohľad nad SIS II (SCG) bola zriadená s cieľom zabezpečiť koordináciu dohľadu nad SIS a zasadá najviac dvakrát ročne. Táto skupina pozostáva z EDPS a zástupcov dozorných orgánov tých členských štátov, ktoré zaviedli SIS II, ako aj Islandu, Lichtenštajnska, Nórska a Švajčiarska, keďže SIS sa vzťahuje aj na nich ako na členov schengenského priestoru⁸⁶⁵. Cyprus, Chorvátsko a Írsko ešte nie sú súčasťou SIS II, a preto sa na SCG zúčastňujú len ako pozorovatelia. V kontexte koordinačnej skupiny pre dohľad EDPS a vnútroštátne dozorné orgány aktívne spolupracujú, pričom si vymieňajú informácie, poskytujú vzájomnú pomoc pri vykonávaní auditov a inšpekcií, vypracúvajú zosúladené návrhy na spoločné riešenia akýchkoľvek problémov a podporujú informovanosť o právach súvisiacich s ochranou údajov⁸⁶⁶. Koordinačná skupina pre dohľad nad SIS II prijíma aj usmernenia na pomoc dotknutým osobám. Jedným z príkladov je príručka na pomoc dotknutým osobám pri uplatňovaní ich práv na prístup⁸⁶⁷.

Výhľad

Európska komisia v roku 2016 vykonala hodnotenie SIS⁸⁶⁸, z ktorého vyplynulo, že v členských štátoch sú zavedené účinné mechanizmy pre dotknuté osoby na účel

864 Nariadenie o SIS II, článok 44 ods. 2.

865 Pozri webovú stránku Európskeho dozorného úradníka pre ochranu údajov o [Schengenskom informačnom systéme](#).

866 Nariadenie o SIS II, článok 46 a rozhodnutie o SIS II, článok 62.

867 Pozri SIS II SCG, *Schengenský informačný systém. Príručka k uplatňovaniu práva na prístup*, ktorá je k dispozícii na webovom sídle EDPS.

868 Európska komisia (2016), *Správa Komisie Európskemu parlamentu a Rade o hodnotení Schengenského informačného systému druhej generácie (SIS II) v súlade s článkom 24 ods. 5, článkom 43 ods. 3 a článkom 50 ods. 5 nariadenia (ES) č. 1987/2006 a článkom 59 ods. 3 a článkom 66 ods. 5 rozhodnutia 2007/533/SVV, COM(2016) 880 final, Brusel, 21. decembra 2016.*

prístupu, opravy, výmazu ich osobných údajov v SIS II alebo na získanie náhrady v súvislosti s nepresnými údajmi. S cieľom zlepšiť efektívnosť a účinnosť SIS II Európska komisia predložila tri návrhy nariadení:

- nariadenie o zriadení, prevádzke a používaní SIS v oblasti hraničných kontrol, ktorým sa zruší nariadenie o SIS II,
- nariadenie o zriadení, prevádzke a používaní SIS v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, ktorým sa okrem iného zruší rozhodnutie o SIS II,
- nariadenie o využívaní SIS na účely návratu neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín.

Dôležité je, že v týchto návrhoch sa umožňuje spracúvanie iných kategórií biometrických údajov – okrem fotografií a odtlačkov prstov, ktoré už sú súčasťou súčasného režimu SIS II. V databáze SIS sa budú ukladať aj odtlačky prstov, odtlačky dlaní a profily DNA. Navyše, zatiaľ čo v nariadení o SIS II a v rozhodnutí o SIS II sa uvádzala možnosť vyhľadávať osoby na základe odtlačkov prstov, v návrhoch je toto vyhľadávanie stanovené ako povinné, ak sa totožnosť osoby nedá zistiť iným spôsobom. Na vyhľadávanie v systéme a identifikáciu osôb sa budú používať podoby tváre, fotografie a odtlačky dlaní, ak to bude technicky možné. Nové pravidlá pre biometrické charakteristiky predstavujú osobitné riziká pre práva jednotlivcov. EDPS vo svojom stanovisku k návrhom Komisie uvádza⁸⁶⁹, že biometrické údaje sú vysoko citlivé a ich zahrnutie do takejto rozsiahlej databázy by malo vychádzať z posúdenia potreby ich začlenenia do SIS na základe dôkazov. Inými slovami, mala by sa preukázať potreba spracúvania nových atribútov. EDPS sa tiež domnieva, že je potrebné ďalej objasniť, aký druh informácií možno zahrnúť do profilu DNA. Keďže profil DNA môže zahŕňať citlivé informácie (najvýznamnejším príkladom by boli informácie o zdravotných problémoch), profily DNA uložené v SIS by mali obsahovať: „len minimálne informácie, ktoré sú nevyhnutne potrebné na identifikáciu nezvestných osôb a výslovne vylučujú zdravotné informácie, rasový pôvod a akékoľvek iné citlivé informácie.“⁸⁷⁰ V návrhoch sa však stanovujú dodatočné záruky na obmedzenie získavania a ďalšieho spracúvania údajov na to, čo je prísne nevyhnutné a potrebné z operačného hľadiska, a prístup je obmedzený na osoby, ktoré osobné údaje potrebujú spracúvať

869 EDPS (2017), Stanovisko Európskeho dozorného úradníka pre ochranu údajov k novému právnemu základu pre Schengenský informačný systém, stanovisko 7/2017, 2. mája 2017.

870 Tamže, bod 22.

z operačného hľadiska⁸⁷¹. Tieto návrhy tiež oprávňujú eu-LISA, aby pravidelne vypracovávala pre členské štáty správy o kvalite údajov s cieľom pravidelne preskúmať zápisy na zabezpečenie kvality údajov⁸⁷².

Vízový informačný systém

Vízový informačný systém (VIS), ktorý tiež prevádzkuje eu-LISA, vznikol s cieľom pomôcť pri vykonávaní spoločnej vízovej politiky EÚ⁸⁷³. VIS umožňuje výmenu údajov o žiadateľoch o udelenie víza medzi schengenskými štátmi prostredníctvom plne centralizovaného systému, ktorý spája veľvyslanectvá schengenských štátov v krajinách, ktoré nie sú členskými štátmi EÚ, s hraničnými priechodmi na vonkajších hraniciach všetkých schengenských štátov. Vo VIS sa spracúvajú údaje týkajúce sa žiadostí o krátkodobé víza na účely návštevy alebo tranzitu cez schengenský priestor. VIS umožňuje pohraničným orgánom, aby na základe biometrických údajov, a najmä odtlačkov prstov, overili, či osoba, ktorá predkladá vízum, je alebo nie je jeho oprávneným držiteľom, a aby identifikovali osoby bez dokladov alebo s podvodnými dokladmi.

V nariadení Európskeho parlamentu a Rady (ES) č. 767/2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (nariadenie o VIS) sa upravujú podmienky a postupy prenosu osobných údajov týkajúcich sa žiadostí o krátkodobé víza. Tento systém dohliada aj na rozhodnutia o žiadostiach vrátane rozhodnutí o zrušení, odvolaní alebo predĺžení platnosti víza⁸⁷⁴. Nariadenie o VIS sa týka najmä údajov o žiadateľovi, jeho vízach, fotografiách, odtlačkoch prstov, súvislostiach s predchádzajúcimi žiadosťami a súboroch so

871 Európska komisia (2016), návrh nariadenia Európskeho parlamentu a Rady o zriadení, prevádzke a používaní Schengenského informačného systému (SIS) v oblasti policajnej spolupráce a justičnej spolupráce v trestných veciach, ktorým sa mení nariadenie (EÚ) č. 515/2014 a ktorým sa zrušuje nariadenie (ES) č. 1986/2006, rozhodnutie Rady 2007/533/SVV a rozhodnutie Komisie 2010/261/EÚ, COM(2016) 883 final, Brusel, 21. decembra 2016.

872 Tamže, s. 15.

873 Rada Európskej únie (2004), rozhodnutie Rady 2004/512/ES z 8. júna 2004, ktorým sa vytvára vízový informačný systém (VIS), Ú. v. EÚ L 213, 2004; nariadenie Európskeho parlamentu a Rady (ES) č. 767/2008 z 9. júla 2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (nariadenie o VIS), Ú. v. EÚ L 218, 2008; Rada Európskej únie (2008), rozhodnutie Rady 2008/633/SVV z 23. júna 2008 o sprístupnení vízového informačného systému (VIS) na nahliadnutie určeným orgánom členských štátov a Europolu na účely predchádzania teroristickým trestným činom a iným závažným trestným činom, ich odhaľovania a vyšetrovania, Ú. v. EÚ L 218, 2008.

874 Nariadenie o VIS, článok 1.

žiadosťami osôb, ktoré ho sprevádzali, alebo údajov o pozývaní osôb⁸⁷⁵. Prístup do VIS na účely zadania, zmeny alebo výmazu údajov je obmedzený výlučne na vízové orgány členských štátov, zatiaľ čo prístup na účely nahliadnutia do údajov je umožnený vízovým orgánom a orgánom oprávneným vykonávať kontroly na hraničných priechodoch na vonkajších hraniciach, imigračným kontrolám a azylovým orgánom.

Za určitých okolností môžu o prístup k údajom zadaným do VIS požiadať príslušné vnútroštátne policajné orgány a Europol na účely prevencie, odhaľovania alebo vyšetrovania teroristických a trestných činov⁸⁷⁶. Keďže VIS bol navrhnutý ako nástroj na podporu vykonávania spoločnej vízovej politiky, zásada obmedzenia účelu, v rámci ktorej sa, ako je vysvetlené v kapitole 3.2, vyžaduje, aby sa osobné údaje spracúvali iba na konkrétne, výslovne a legitímne účely, pričom spracúvanie musí byť primerané, relevantné a nesmie byť neúmerne vo vzťahu k účelom, na ktoré sa údaje spracúvajú, by bola porušená, ak by sa VIS stal nástrojom na presadzovanie práva. Z tohto dôvodu sa vnútroštátnym orgánom presadzovania práva a Europolu neposkytuje bežný prístup do databázy VIS. Prístup sa môže udeliť len na individuálnom základe a spájajú sa s ním prísne záruky. Podmienky a záruky týkajúce sa sprístupnenia VIS a nahliadnutia do VIS pre tieto orgány sa upravujú v rozhodnutí Rady 2008/633/SVV.⁸⁷⁷

V nariadení o VIS sa okrem toho stanovujú práva dotknutých osôb. Ide o:

- Právo byť informovaný zodpovedným členským štátom o totožnosti a kontaktných údajoch prevádzkovateľa, ktorý má na starosti spracúvanie osobných údajov v rámci tohto členského štátu, účeloch, na ktoré sa ich osobné údaje budú spracúvať v rámci VIS, kategóriách osôb, ktorým sa údaje môžu poskytnúť (príjemcovia), a lehote uchovávanía údajov. Žiadatelia o udelenie víza musia byť okrem toho informovaní o tom, že získavanie ich osobných údajov v rámci VIS je povinné na posúdenie ich žiadosti, pričom členské štáty ich musia tiež informovať o existencii ich práva na prístup k ich údajom, práva požadovať ich opravu alebo vymazanie a o postupoch, ktoré im umožnia vykonávať tieto práva⁸⁷⁸.

875 Nariadenie Európskeho parlamentu a Rady (ES) č. 767/2008 o vízovom informačnom systéme (VIS) a výmene údajov o krátkodobých vízach medzi členskými štátmi (nariadenie o VIS), Ú. v. EÚ L 218, 2008, článok 5.

876 Rada Európskej únie (2008), rozhodnutie Rady 2008/633/SVV z 23. júna 2008 o sprístupnení vízového informačného systému (VIS) na nahliadnutie určeným orgánom členských štátov a Europolu na účely predchádzania teroristickým trestným činom a iným závažným trestným činom, ich odhaľovania a vyšetrovania, Ú. v. EÚ L 218, 2008.

877 Tamže.

878 Nariadenie o VIS, článok 37.

- Právo na prístup k osobným údajom, ktoré sa ich týkajú a ktoré boli zaznamenané vo VIS⁸⁷⁹.
- Právo na opravu nesprávnych údajov⁸⁸⁰.
- Právo na vymazanie nezákonne uložených údajov⁸⁸¹.

Na zabezpečenie dohľadu nad VIS bola vytvorená koordinačná skupina pre dohľad nad VIS (VIS SCG). Skladá sa zo zástupcov EDPS a vnútroštátnych orgánov dohľadu, ktoré sa schádzajú dvakrát ročne. Túto skupinu tvoria zástupcovia 28 členských štátov EÚ a Islandu, Lichtenštajnska, Nórska a Švajčiarska.

Eurodac

Eurodac znamená Európsky systém na porovnávanie odtlačkov prstov žiadateľov o azyl⁸⁸². Ide o centralizovaný systém obsahujúci údaje o odtlačkoch prstov štátnych príslušníkov tretích krajín, ktorí žiadajú o azyl v niektorom z členských štátov EÚ⁸⁸³. Systém funguje od januára 2003, kedy bolo prijaté nariadenie Rady č. 2725/2000, prepracované znenie sa začalo uplatňovať v roku 2015. Účelom systému je predovšetkým pomôcť určiť konkrétny členský štát, ktorý by mal zodpovedať za preskúmanie konkrétnej žiadosti o azyl podľa nariadenia Rady (ES) č. 604/2013. V tomto nariadení sa stanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov

879 Tamže, článok 38 ods. 1.

880 Tamže, článok 38 ods. 2.

881 Tamže, článok 38 ods. 2.

882 Pozri [webovú stránku Európskeho dozorného úradníka pre ochranu údajov o systéme Eurodac](#).

883 Nariadenie Rady (ES) č. 2725/2000 z 11. decembra 2000, ktoré sa týka zriadenia systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie Dublinského dohovoru, Ú. v. ES L 316, 2000; nariadenie Rady (ES) č. 407/2002 z 28. februára 2002 ustanovujúce určité pravidlá na vykonávanie nariadenia (ES) č. 2725/2000, ktoré sa týka zriadenia systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie Dublinského dohovoru, Ú. v. ES L 62, 2002 (nariadenia Eurodac), nariadenie Európskeho Parlamentu a Rady (EÚ) č. 603/2013 z 26. júna 2013 o zriadení systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie nariadenia (EÚ) č. 604/2013, ktorým sa ustanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov, a o žiadostiach orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva a o zmene nariadenia (EÚ) č. 1077/2011, ktorým sa zriaďuje Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti, Ú. v. EÚ L 180, 2013, s. 1 (prepracované znenie nariadenia Eurodac).

(nariadenie Dublin III)⁸⁸⁴. Osobné údaje v systéme Eurodac slúžia najmä na uľahčenie uplatňovania nariadenia Dublin III⁸⁸⁵.

Vnútroštátne orgány presadzovania práva a Europol môžu porovnávať odtlačky prstov súvisiace s vyšetrovaním trestných činov s odtlačkami prstov v systéme Eurodac, ale len na účely prevencie, odhaľovania alebo vyšetrovania teroristických alebo iných závažných trestných činov. Keďže systém Eurodac bol navrhnutý ako nástroj na podporu vykonávania azylovej politiky EÚ, a nie ako nástroj presadzovania práva, orgány presadzovania práva majú prístup do databázy len v osobitných prípadoch, za konkrétnych okolností a za prísnych podmienok⁸⁸⁶. Na ďalšie použitie údajov na účely presadzovania práva sa uplatňuje smernica o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní, zatiaľ čo údaje používané hlavne na uľahčenie uplatňovania nariadenia Dublin III sú chránené podľa všeobecného nariadenia o ochrane údajov. Osobné údaje, ktoré získa členský štát alebo Europol podľa prepracovaného znenia nariadenia Eurodac, je zakázané ďalej odosielať akejkoľvek tretej krajine, medzinárodnej organizácii alebo súkromnému subjektu usadenému v EÚ alebo mimo nej⁸⁸⁷.

Systém Eurodac tvorí centrálna jednotka, prevádzkovaná eu-LISA, určená na uchovávanie a porovnávanie odtlačkov prstov, a systém elektronického poskytovania údajov medzi členskými štátmi a centrálnou databázou. Členské štáty odoberú a poskytnú odtlačky prstov každej osoby vo veku aspoň 14 rokov, ktorá požiada o azyl na ich území, a každého štátneho príslušníka tretej krajiny alebo osoby bez štátnej príslušnosti vo veku aspoň 14 rokov, ktorá bola zadržaná pri nelegálnom prechode ich vonkajších hraníc. Členské štáty môžu tiež odobrať a poskytnúť odtlačky prstov štátneho príslušníka tretej krajiny alebo každej osoby bez štátnej príslušnosti, u ktorej sa zistí, že pobýva na ich území bez povolenia.

Hoci každý členský štát môže nahliadnuť do systému Eurodac a požiadať o porovnanie údajov o odtlačkoch prstov, iba členský štát, ktorý odobral odtlačky prstov a odoslal ich centrálnej jednotke, má právo tieto údaje zmeniť, a to tak, že ich opraví,

884 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 604/2013 z 26. júna 2013, ktorým sa stanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov, Ú. v. EÚ L 180, 2013 (nariadenie Dublin III).

885 Prepracované znenie nariadenia Eurodac, Ú. v. EÚ L 180, 2013, s. 1, článok 1 ods. 1.

886 Tamže, článok 1 ods. 2.

887 Tamže, článok 35.

doplní alebo vymaže⁸⁸⁸. eu-LISA vedie záznamy o každom spracúvaní údajov na účely monitorovania ochrany údajov a zaistenia bezpečnosti údajov⁸⁸⁹. Národné dozorné orgány pomáhajú dotknutým osobám a radia im v súvislosti s výkonom ich práv⁸⁹⁰. Získavanie a poskytovanie údajov o odtlačkoch prstov podlieha súdnemu preskúmaniu zo strany vnútroštátnych súdov⁸⁹¹. Všetky spracovateľské činnosti v centrálnom systéme, ktorý riadi eu-LISA, týkajúce sa systému Eurodac⁸⁹² sa vykonávajú v súlade s nariadením o ochrane údajov v inštitúciách EÚ⁸⁹³ a pod dohľadom EDPS. Ak osoba utrpela škodu v dôsledku nezákonnej spracovateľskej operácie alebo akéhokoľvek konania v rozpore s nariadením Eurodac, má nárok na náhradu škody od členského štátu zodpovedného za škodu⁸⁹⁴. Je však potrebné zdôrazniť, že žiadatelia o azyl sú obzvlášť zraniteľnou skupinou ľudí, ktorí často majú za sebou dlhé a riskantné cestovanie. Z dôvodu ich zraniteľnosti a nejistej situácie, v ktorej sa často nachádzajú počas posudzovania svojej žiadosti o azyl, sa v praxi uplatňovanie ich práv vrátane práva na odškodnenie môže ukázať ako zložité.

Aby členské štáty mohli využívať Eurodac na účely presadzovania práva, musia určiť orgány, ktoré budú mať právo požiadať o prístup, ako aj orgány, ktoré overia, či sú žiadosti o porovnanie oprávnené⁸⁹⁵. Prístup vnútroštátnych orgánov a Europolu k údajom o odtlačkoch prstov v systéme Eurodac podlieha veľmi prísny podmienkam. Po porovnaní údajov s údajmi v iných dostupných informačných systémoch, ako sú vnútroštátne databázy odtlačkov prstov a VIS, musí žiadajúci orgán predložiť odôvodnenú elektronickú žiadosť. Musí existovať prevažujúca obava z hľadiska verejnej bezpečnosti, na základe ktorej je porovnanie primerané. Porovnanie musí byť skutočne potrebné, musí sa týkať konkrétneho prípadu a musia existovať opodstatnené dôvody domnievať sa, že toto porovnanie významne prispeje k predchádzaniu niektorému z príslušných trestných činov, jeho odhaleniu alebo vyšetrovaniu, najmä ak existuje dôvodné podozrenie, že podozrivý, páchatel alebo obeť teroristického trestného činu alebo iného závažného trestného činu patrí do kategórie, pri

888 Tamže, článok 27.

889 Tamže, článok 28.

890 Tamže, článok 29.

891 Tamže, článok 29.

892 Prepracované znenie nariadenia o systéme Eurodac, Ú. v. EÚ L 180, 2013, s. 1, článok 31.

893 Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov, Ú. v. ES L 8, 2001.

894 Tamže, článok 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination“, *Baltic Journal of European Studies Tallinn University of Technology*, zv. 5, č. 2, s. 108 – 129.

ktorej sa získavajú odtlačky prstov v rámci systému Eurodac. Porovnanie sa musí vykonať výlučne s údajmi o odtlačkoch prstov. Europol musí takisto získať povolenie od členského štátu, ktorý údaje o odtlačkoch prstov získal.

Osobné údaje uchovávané v systéme Eurodac, ktoré sa týkajú žiadateľov o azyl, sa uchovávajú 10 rokov od dátumu odobratia odtlačkov prstov, okrem prípadov, keď dotknutá osoba získa občianstvo niektorého členského štátu EÚ. V takom prípade sa údaje musia okamžite vymazať. Údaje o cudzích štátnych príslušníkoch zadržaných pri nepovolenom prekročení vonkajšej hranice sa uchovávajú 18 mesiacov. Tieto údaje sa musia vymazať bezprostredne po tom, ako sa dotknutej osobe udelí povolenie na pobyt, ako dotknutá osoba opustí územie EÚ alebo získa občianstvo niektorého členského štátu. Údaje o osobách, ktorým bol udelený azyl, zostávajú dostupné na porovnanie počas troch rokov v kontexte predchádzania teroristickým trestným činom a iným závažným trestným činom, ich odhaľovania a vyšetrovania.

Systém Eurodac využívajú okrem všetkých členských štátov EÚ aj Island, Nórsko, Lichtenštajnsko a Švajčiarsko, a to na základe medzinárodných dohôd.

Koordinačná skupina pre dohľad nad systémom Eurodac (Eurodac SCG) bola vytvorená na zabezpečenie dohľadu nad systémom Eurodac. Skladá sa zo zástupcov EDPS a vnútroštátnych orgánov dohľadu, ktoré sa schádzajú dvakrát ročne. Táto skupina pozostáva zo zástupcov 28 členských štátov EÚ a Islandu, Lichtenštajnska, Nórska a Švajčiarska⁸⁹⁶.

Výhľad

V máji 2016 Komisia v rámci reformy zameranej na zlepšenie fungovania spoločného európskeho azylového systému (CEAS) vydala návrh nového prepracovaného nariadenia Eurodac⁸⁹⁷. Navrhované prepracovanie je dôležité, pretože sa ním výrazne rozšíri rozsah pôsobnosti pôvodnej databázy Eurodac. Systém Eurodac bol pôvodne vytvorený na podporu vykonávania CEAS tým, že poskytoval dôkazy vo

896 Pozri [webovú stránku Európskeho dozorného úradníka pre ochranu údajov o systéme Eurodac](#).

897 Európska komisia, návrh nariadenia Európskeho parlamentu a Rady o zriadení systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie [nariadenia (EÚ) č. 604/2013, ktorým sa ustanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov, na zistenie totožnosti neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín alebo osôb bez štátnej príslušnosti a o zriadnutí orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva (prepracované znenie), COM(2016) 272 final, 4. mája 2016.

forme odtlačkov prstov umožňujúce určiť, ktorý členský štát je zodpovedný za posúdenie žiadosti o azyl podanej v EÚ. Navrhovaným prepracovaným znením sa rozšíri rozsah databázy s cieľom uľahčiť návrat migrantov, ktorí nezákonne prekročili hranice⁸⁹⁸. Vnútroštátne orgány budú môcť nahliadnuť do databázy na účely identifikácie štátnych príslušníkov tretích krajín, ktorí sa zdržiavajú v EÚ alebo ktorí vstúpili do EÚ v súvislosti s nezákonným prekročením hraníc, s cieľom získať dôkazy, ktoré by členským štátom pomohli pri návrate týchto osôb. Okrem toho, hoci podľa právneho režimu platného v súčasnosti sa vyžaduje len získavanie a uchovávanie odtlačkov prstov, v návrhu sa zavádza získavanie podob tváre⁸⁹⁹ fyzických osôb, čo je ďalší typ biometrických údajov. V návrhu by sa znížil aj minimálny vek detí, ktorým sa môžu odoberať biometrické údaje – na šesť rokov⁹⁰⁰ namiesto 14 rokov, čo je minimálny vek podľa nariadenia z roku 2013. Rozšírený rozsah pôsobnosti návrhu znamená, že bude predstavovať zásah do práv na súkromie a ochranu údajov väčšieho počtu osôb, ktoré môžu byť zaradené do databázy. Na vyváženie tohto vplyvu sa návrh a pozmeňujúce návrhy výboru Európskeho parlamentu LIBE⁹⁰¹ usilujú o posilnenie požiadaviek na ochranu údajov. V čase prípravy tejto príručky prebiehali rokovania o tomto návrhu v Parlamente a Rade.

EUROSUR

Cieľom európskeho systému hraničného dozoru (EUROSUR)⁹⁰² je posilniť kontrolu vonkajších hraníc schengenského priestoru prostredníctvom zisťovania a prevencie nelegálneho prisťahovalectva a cezhraničnej trestnej činnosti a boja proti nim. Tento

898 Pozri dôvodovú správu k návrhu, s. 3.

899 Európska komisia, návrh nariadenia Európskeho parlamentu a Rady o zriadení systému Eurodac na porovnávanie odtlačkov prstov pre účinné uplatňovanie [nariadenia (EÚ) č. 604/2013, ktorým sa ustanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov, na zistenie totožnosti neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín alebo osôb bez štátnej príslušnosti a o žiadostiach orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva (prepracované znenie), COM(2016) 272 final, 4. mája 2016, článok 2 ods. 1.

900 Tamže, článok 2 ods. 2.

901 Európsky parlament, *správa o návrhu nariadenia Európskeho parlamentu a Rady o zriadení systému Eurodac na porovnávanie odtlačkov prstov na účinné uplatňovanie [nariadenia (EÚ) č. 604/2013, ktorým sa ustanovujú kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o medzinárodnú ochranu podanej štátnym príslušníkom tretej krajiny alebo osobou bez štátnej príslušnosti v jednom z členských štátov], na zistenie totožnosti neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín alebo osôb bez štátnej príslušnosti a o žiadostiach orgánov členských štátov na presadzovanie práva a Europolu o porovnanie s údajmi v systéme Eurodac na účely presadzovania práva (prepracované znenie)*, PE 597.620v03-00, 9. júna 2017.

902 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1052/2013 z 22. októbra 2013, ktorým sa zriaďuje európsky systém hraničného dozoru (EUROSUR), Ú. v. EÚ L 295, 2013.

systém súži na zlepšenie výmeny informácií a operačnej spolupráce medzi národnými koordináčnymi centrami a agentúrou Frontex, čo je agentúra EÚ zodpovedná za prípravu a realizáciu novej koncepcie integrovaného riadenia hraníc⁹⁰³. K všeobecným cieľom patrí:

- znížiť počet neregulárnych migrantov, ktorí vstúpia na územie EÚ a zostanú neodhalení,
- znížiť počet úmrtí neregulárnych migrantov, a to záchranou väčšieho počtu životov na mori,
- zvýšiť vnútornú bezpečnosť EÚ ako celku, a to príspevom k prevencii cezhraničnej trestnej činnosti⁹⁰⁴.

Systém EUROSUR začal fungovať 2. decembra 2013 vo všetkých členských štátoch s vonkajšími hranicami a od 1. decembra 2014 v ostatných členských štátoch. Nariadenie sa týka dozoru nad suchozemskými a morskými vonkajšími hranicami a vzdušnými hranicami členských štátov. V rámci systému EUROSUR dochádza k výmene a spracúvaniu osobných údajov vo veľmi obmedzenom rozsahu, keďže členské štáty a agentúra Frontex majú právo vymieňať si len identifikačné čísla lodí. V rámci systému EUROSUR sa vymieňajú operačné informácie, ako je poloha hlíadok a mimoriadnych udalostí, a výmena informácií vo všeobecnosti nemôže zahŕňať osobné údaje⁹⁰⁵. Vo výnimočných prípadoch, keď sa v rámci systému EUROSUR vymieňajú osobné údaje, sa v nariadení stanovuje, že všeobecný právny rámec EÚ v oblasti ochrany údajov sa uplatňuje v plnom rozsahu⁹⁰⁶.

Systém EUROSUR teda zabezpečuje právo na ochranu údajov tým, že uvádza, že výmeny osobných údajov musia byť v súlade s kritériami a so zárukami

903 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/1624 zo 14. septembra 2016 o európskej pohraničnej a pobrežnej stráž, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) 2016/399 a ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 863/2007, nariadenie Rady (ES) č. 2007/2004 a rozhodnutie Rady 2005/267/ES, Ú. v. EÚ L 251.

904 Pozri tiež: Európska komisia (2008), *oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Preskúmanie vytvorenia Európskeho systému hraničného dozoru (EUROSUR)* COM(2008) 68 final, Brusel, 13. februára 2008; Európska komisia (2011), *Posúdenie vplyvu, sprievodný dokument k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európsky systém hraničného dozoru (EUROSUR)*, pracovný dokument útvarov Komisie, SEK (2011) 1536 v konečnom znení, Brusel, 12. decembra 2011, s. 18.

905 Európska komisia, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29. novembra 2013.

906 Nariadenie č. 1052/2013, odôvodnenie 13 a článok 13.

stanovenými v smernici o ochrane údajov pre policajné orgány a orgány činné v trestnom konaní a vo všeobecnom nariadení o ochrane údajov⁹⁰⁷.

Colný informačný systém

Ďalším dôležitým spoločným informačným systémom zriadeným na úrovni EÚ je colný informačný systém (CIS)⁹⁰⁸. V rámci zriadenia vnútorného trhu boli zrušené všetky kontroly a formality týkajúce sa tovaru prevážaného na území EÚ, čo viedlo ku zvýšeniu rizika podvodov. Toto riziko sa vyvážilo zintenzívnením spolupráce medzi colnými správami jednotlivých členských štátov. Účelom CIS je pomáhať členským štátom pri prevencii, vyšetrovaní a stíhaní závažných porušení vnútroštátnych a európskych právnych predpisov v oblasti ciel a poľnohospodárstva. CIS bol vytvorený na základe dvoch právnych aktov prijatých na rôznych právnych základoch: nariadenie Rady (ES) č. 515/97 sa týka spolupráce medzi rôznymi vnútroštátnymi správnymi orgánmi v boji proti podvodom v rámci colnej únie a spoločnej poľnohospodárskej politiky, pričom cieľom rozhodnutia Rady 2009/917/SVV je pomáhať pri predchádzaní, vyšetrovaní a trestnom stíhaní závažných porušení colných predpisov. To znamená, že CIS sa netýka len presadzovania práva.

Informácie uvedené v CIS zahŕňajú osobné údaje týkajúce sa komodít, dopravných prostriedkov, podnikov, osôb, tovarov a hotovosti, ktoré boli zadržané, zachytené alebo skonfiškované. Kategórie údajov, ktoré možno spracúvať, sú jasne vymedzené a zahŕňajú mená, štátnu príslušnosť, pohlavie, miesto a dátum narodenia dotknutých osôb, dôvod zahrnutia ich údajov do systému a evidenčné číslo dopravného prostriedku⁹⁰⁹. Tieto informácie sa smú používať výlučne na účely kontrol, oznamovania alebo vykonávania konkrétnych inšpekcií alebo na strategické či operačné analýzy týkajúce sa osôb podozrivých z porušenia colných ustanovení.

Prístup do CIS je povolený vnútroštátnym colným a daňovým orgánom a orgánom v oblasti poľnohospodárstva a verejného zdravia, policajným orgánom, ako aj Europolu a Eurojustu.

⁹⁰⁷ Tamže, odôvodnenie 13 a článok 13.

⁹⁰⁸ Rada Európskej únie (1995), Akt Rady z 26. júla 1995 o vypracovaní Dohovoru o využívaní informačných technológií na colné účely, Ú. v. ES C 316, 1995, zmenený nariadením Rady Európskej únie (2009), nariadenie Rady (ES) č. 515/97 z 13. marca 1997 o vzájomnej pomoci medzi správnymi orgánmi členských štátov a o spolupráci medzi správnymi orgánmi členských štátov a Komisiou pri zabezpečovaní riadneho uplatňovania predpisov o colných a poľnohospodárskych záležitostiach, rozhodnutie Rady 2009/917/SVV z 30. novembra 2009 o využívaní informačných technológií na colné účely (rozhodnutie o CIS), Ú. v. EÚ L 323, 2009.

⁹⁰⁹ Pozri rozhodnutie o CIS, články 24, 25 a 28.

Spracúvanie osobných údajov musí byť v súlade s osobitnými pravidlami stanovenými v nariadení č. 515/1997 a rozhodnutí Rady 2009/917/SVV, ako aj ustanoveniami všeobecného nariadenia o ochrane údajov, nariadenia o ochrane údajov inštitúciami EÚ, modernizovaného Dohovoru č. 108 a odporúčania v oblasti polície. EDPS je zodpovedný za dohľad nad tým, že v rámci CIS sa dodržiava nariadenie (ES) č. 45/2001. Najmenej raz za rok zvolá stretnutie so všetkými vnútroštátnymi dozornými orgánmi pre ochranu údajov s právomocou v oblasti otázok dohľadu v súvislosti so systémom CIS.

Interoperabilita medzi informačnými systémami EÚ

Riadenie migrácie, integrované riadenie vonkajších hraníc EÚ a boj proti terorizmu a cezhraničnej trestnej činnosti predstavujú dôležité výzvy a v globalizovanom svete sú tieto oblasti čoraz komplexnejšie. V posledných rokoch EÚ pracuje na novom komplexnom prístupe k ochrane a udržiavaniu bezpečnosti bez toho, aby boli ohrozené hodnoty a základné slobody EÚ. Pri tomto úsilí je kľúčová účinná výmena informácií medzi vnútroštátnymi orgánmi presadzovania práva, ako aj medzi členskými štátmi a príslušnými agentúrami EÚ⁹¹⁰. Existujúce informačné systémy EÚ v oblasti riadenia hraníc a vnútornej bezpečnosti majú svoje príslušné ciele, inštitucionálne štruktúry, dotknuté osoby a používateľov. EÚ sa usiluje prekonať nedostatky v oblasti fungovania roztriešteného riadenia údajov EÚ medzi rôznymi informačnými systémami, ako sú SIS II, VIS a Eurodac, pričom v tejto oblasti skúma potenciál interoperability⁹¹¹. Hlavným cieľom je zabezpečiť, aby príslušné policajné, colné a súdne orgány mali systematicky k dispozícii potrebné informácie na plnenie svojich povinností, pri zachovaní rovnováhy, pokiaľ ide o práva na súkromie, ochranu údajov a ďalšie základné práva.

910 Európska komisia (2016), oznámenie Komisie Európskemu parlamentu a Rade: Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť, COM (2016) 205 final, Brusel, 6. apríla 2016, Európska komisia (2016), oznámenie Komisie Európskemu parlamentu, Európskej rade a Rade: Posilnenie bezpečnosti vo svete mobility: lepšia výmena informácií v boji proti terorizmu a lepšie chránené vonkajšie hranice, COM (2016) 602 final, Brusel, 14. septembra 2016, Európska komisia (2016), návrh nariadenia Európskeho parlamentu a Rady o používaní Schengenského informačného systému na účely návratu neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín. Pozri aj oznámenie Komisie Európskemu parlamentu, Európskej rade a Rade: Siedma správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej únie, COM (2017) 261 final, Brusel, 16. mája 2017.

911 Rada Európskej únie (2005), Haagsky program: posilňovanie slobody, bezpečnosti a spravodlivosti v Európskej únii, Ú. v. EÚ C 53, 2005; Európska komisia (2010), oznámenie Komisie Európskemu parlamentu a Rade: Prehľad o riadení informácií v oblasti slobody, bezpečnosti a spravodlivosti, KOM (2010) 385 v konečnom znení; Európska komisia (2016), oznámenie Komisie Európskemu parlamentu a Rade: Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť, COM(2016) 205 final, Brusel, 6. apríla 2016, Európska komisia (2016), rozhodnutie Komisie zo 17. júna 2016, ktorým sa zriaďuje expertná skupina na vysokej úrovni pre informačné systémy a interoperabilitu, Ú. v. EÚ C 257, 2016.

Interoperabilita je schopnosť informačných systémov vymieňať si údaje a umožniť výmenu informácií⁹¹². Táto výmena nesmie ohrozovať nevyhnutne prísne pravidlá o prístupe k údajom a ich využívaní, ktoré sú zaručené vo všeobecnom nariadení o ochrane údajov, smernici o ochrane údajov pre orgány polície a trestného súdnictva, Charte základných práv EÚ a všetkých ostatných príslušných pravidlách. Nijaké integrované riešenie pre riadenie údajov nesmie ovplyvňovať zásady obmedzenia účelu, špecificky navrhutej ochrany údajov alebo štandardnej ochrany údajov⁹¹³.

Okrem zlepšenia funkcií troch hlavných informačných systémov – SIS II, VIS a Eurodac – Komisia navrhla zriadenie štvrtého centralizovaného systému riadenia hraníc, zameraného na štátnych príslušníkov tretích krajín: systém vstup/výstup (EES)⁹¹⁴, ktorý sa má zaviesť do roku 2020⁹¹⁵. Komisia takisto predložila návrh na zriadenie Európskeho systému pre cestovné informácie a povolenia (ETIAS⁹¹⁶), v ktorom sa budú zhromažďovať informácie o osobách cestujúcich bez víz do EÚ s cieľom umožniť vopred vykonávať bezpečnostné kontroly v prípadoch migrácie v súvislosti s nezákonným prekročením hraníc.

912 Európska komisia (2016), oznámenie Komisie Európskemu parlamentu a Rade: Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť; COM (2016) 205 final, Brusel, 6. apríla 2016, s. 14.

913 Tamže, s. 4 – 5.

914 Európska komisia (2016), návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje systém vstup/výstup (EES) na zaznamenávanie údajov o vstupe a výstupe a odopretí vstupe v prípade štátnych príslušníkov tretích krajín prekračujúcich vonkajšie hranice členských štátov Európskej únie a ktorým sa stanovujú podmienky prístupu do systému vstup/výstup na účely presadzovania práva a ktorým sa mení nariadenie (ES) č. 767/2008 a nariadenie (EÚ) č. 1077/2011, COM(2016) 194 final, Brusel, 6. apríla 2016.

915 Európska komisia (2016), oznámenie Komisie Európskemu parlamentu a Rade: Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť; COM (2016) 205 final, Brusel, 6. apríla 2016, s. 5.

916 Európska komisia (2016), návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje európsky systém pre cestovné informácie a povolenia (ETIAS) a ktorým sa menia nariadenia (EÚ) č. 515/2014, (EÚ) 2016/399, (EÚ) 2016/794 a (EÚ) 2016/1624, COM(2016) 731 final, 16. novembra 2016.

9

Osobitné druhy údajov a príslušné pravidlá ochrany údajov

EÚ	Zahrnuté témy	RE
Všeobecné nariadenie o ochrane údajov Smernica o súkromí a elektronických komunikáciách	Elektronické komunikácie	Modernizovaný Dohovor č. 108 Odporúčanie o telekomunikačných službách
Všeobecné nariadenie o ochrane údajov, článok 88	Pracovnoprávne vzťahy	Modernizovaný Dohovor č. 108 Odporúčanie o údajoch o zamestnaní ESLP, <i>Copland/Spojené kráľovstvo</i> , č. 62617/00, 2007
Všeobecné nariadenie o ochrane údajov, článok 9 ods. 2 písm. h) a i)	Zdravotné údaje	Modernizovaný Dohovor č. 108 Odporúčanie o zdravotných údajoch ESLP, <i>Z/Fínsko</i> , č. 22009/93, 1997
Nariadenie o klinickom skúšaní liekov	Klinické skúšanie liekov	
Všeobecné nariadenie o ochrane údajov, článok 6 ods. 4, článok 89	Štatistiky	Modernizovaný Dohovor č. 108 Odporúčanie o štatistických údajoch
Nariadenie (ES) č. 223/2009 o európskej štatistike SDEÚ, C-524/06, <i>Huber/Bundesrepublik Deutschland</i> [VK], 2008	Oficiálne štatistiky	Modernizovaný Dohovor č. 108 Odporúčanie o štatistických údajoch

EÚ	Zahrnuté témy	RE
Smernica 2014/65/EÚ o trhoch s finančnými nástrojmi Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov Nariadenie (ES) č. 1060/2009 o ratingových agentúrach Smernica 2007/64/ES o platobných službách na vnútornom trhu	Finančné údaje	Modernizovaný Dohovor č. 108 Odporúčanie 90 (19) o spracúvaní osobných údajov používaných na platby a iné súvisiace operácie ESLP, <i>Michaud/</i> Francúzsko, č. 12323/11, 2012

Vo viacerých prípadoch boli na európskej úrovni prijaté osobitné právne nástroje na podrobnejšie uplatňovanie všeobecných pravidiel modernizovaného Dohovoru č. 108 alebo všeobecného nariadenia o ochrane údajov pre konkrétne situácie.

9.1. Elektronické komunikácie

Hlavné body

- Osobitné pravidlá týkajúce sa ochrany údajov v oblasti telekomunikácií, s osobitným zreteľom na telefonické služby, sú uvedené v odporúčaní Rady Európy z roku 1995.
- Spracúvanie osobných údajov v súvislosti s poskytovaním telekomunikačných služieb na úrovni EÚ je upravené smernicou o súkromí a elektronických komunikáciách.
- Dôverynosť elektronických komunikácií sa týka nielen obsahu komunikácie, ale aj meta-údajov, napríklad informácií o tom, kto s kým komunikoval, kedy a ako dlho, ako aj lokalizačných údajov, napríklad odkiaľ boli údaje komunikované.

Komunikačné siete sa vyznačujú vyšším potenciálom neoprávneného zasahovania do osobnej sféry používateľov, keďže poskytujú dodatočné technické možnosti na odpočúvanie a sledovanie komunikácie realizovanej v týchto sieťach. Preto sa považovalo za nevyhnutné prijať osobitné nariadenia o ochrane údajov s cieľom riešiť konkrétne riziká pre používateľov komunikačných služieb.

V roku 1995 **RE** vydala odporúčanie na ochranu údajov v oblasti telekomunikácií, s osobitným zreteľom na telefonické služby⁹¹⁷. Podľa tohto odporúčania by sa účely získavania a spracúvania údajov v kontexte telekomunikácií mali obmedziť na: pripojenie používateľa k sieti, sprístupnenie konkrétnych telekomunikačných služieb, fakturáciu, overenie, zaistenie optimálnej technickej prevádzky a rozvoj siete a služby.

Osobitná pozornosť bola venovaná používaniu komunikačných sietí na zasielanie priamych marketingových správ. Vo všeobecnosti platí, že priame marketingové správy nesmú byť adresované účastníkom, ktorí výslovne odmietli možnosť doručovania marketingových správ. Automatizované telefonické zariadenia na prenos vopred zaznamenaných reklamných správ sa môžu používať len v prípade, že účastník poskytol svoj výslovný súhlas. Podrobné pravidlá v tejto oblasti sú uvedené vo vnútroštátnych právnych predpisoch.

Pokiaľ ide o **právny rámec EÚ**, po prvom pokuse v roku 1997 bola v roku 2002 prijatá a v roku 2009 zmenená smernica o súkromí a elektronických komunikáciách. Cieľom bolo doplniť a spresniť ustanovenia predošlej smernice o ochrane údajov pre telekomunikačný sektor⁹¹⁸.

Uplatňovanie smernice o súkromí a elektronických komunikáciách je obmedzené na komunikačné služby vo verejných elektronických sieťach.

V smernici o súkromí a elektronických komunikáciách sa rozlišujú tri hlavné kategórie údajov vytvorených v rámci komunikácie:

- údaje predstavujúce obsah správ odoslaných v priebehu komunikácie; tieto údaje sú prísne dôverné,

917 Rada Európy, Výbor ministrov (1995), Odporúčanie členským štátom Rec(95)4 o ochrane osobných údajov v oblasti telekomunikačných služieb, s osobitným zreteľom na telefonické služby, 7. februára 1995.

918 Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 2002, zmenená smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, Ú. v. EÚ L 337, 2009.

- údaje nevyhnutne potrebné na nadviazanie a udržanie komunikácie, tzv. metaúdaje, v smernici nazývané aj prevádzkové údaje, napríklad informácie o komunikujúcich partneroch, čase a dĺžke komunikácie,
- metaúdaje zahŕňajú údaje, ktoré sa konkrétne týkajú umiestnenia komunikačného zariadenia, tzv. lokalizačné údaje – sú to zároveň údaje o tom, kde sa používateľ komunikačných zariadení nachádza, a majú osobitný význam pre používateľov mobilných komunikačných zariadení.

Poskytovateľ služieb môže používať prevádzkové údaje len pri fakturácii a technikom poskytovaní služby. Tieto údaje však môžu byť so súhlasom dotknutej osoby poskytnuté ďalším prevádzkovateľom ponúkajúcim služby s pridanou hodnotou, napríklad poskytovanie informácií súvisiacich s miestom, na ktorom sa používateľ nachádza, napr. kde je najbližšia stanica metra alebo lekáreň či aká je predpoveď počasia pre dané miesto.

Podľa článku 15 smernice o ePrivacy iný prístup k údajom o komunikácii v elektronických sieťach musí spĺňať požiadavky na oprávnené zasahovanie do práva na ochranu údajov stanovené v článku 8 ods. 2 ECHR a potvrdené v Charte základných práv EÚ v článkoch 8 a 52. Takýto prístup by mohol zahŕňať prístup na účely vyšetrovania trestných činov.

Zmenami smernice o súde súkromí a elektronických komunikáciách z roku 2009⁹¹⁹ sa zaviedli tieto ustanovenia:

- Obmedzenia týkajúce sa zasielania e-mailov na priame marketingové účely boli rozšírené na služby zasielania krátkych textových správ, multimediálnych správ a ďalšie podobné druhy aplikácií; marketingové e-maily sú zakázané, pokiaľ používateľ neposkytol predchádzajúci súhlas. Bez súhlasu používateľa je možné zasielať marketingové e-maily len bývalým zákazníkom, ak sprístupnili svoju e-mailovú adresu a nenamietajú proti zasielaniu e-mailov.

⁹¹⁹ Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, Ú. v. EÚ L 337, 2009.

- Členským štátom bola uložená povinnosť poskytnúť opravné prostriedky proti porušeniu zákazu nevyžiadanej komunikácie⁹²⁰.
- Nie je už možné používanie súborov cookies – softvéru, ktorý monitoruje a zaznamenáva činnosti používateľa počítača –, bez súhlasu používateľa počítača. Vo vnútroštátnych právnych predpisoch by sa malo v záujme zaistenia dostatočnej ochrany podrobnejšie upraviť, ako by sa mal súhlas poskytovať a získavať⁹²¹.

Ak v dôsledku neoprávneného prístupu, straty alebo zničenia údajov dôjde k porušeniu ochrany údajov, ihneď o tom musí byť informovaný príslušný dozorný orgán. Ak je dôsledkom porušenia ochrany údajov možné poškodenie účastníkov, musia byť informovaní aj účastníci⁹²².

V smernici o uchovávaní údajov⁹²³ sa vyžadovalo, aby poskytovatelia komunikačných služieb uchovávali metaúdaje. SDEÚ však túto smernicu zrušil (podrobnejšie informácie sa uvádzajú v [oddiele 8.3](#)).

Výhľad

V januári 2017 Európska komisia prijala nový návrh nariadenia o ePrivacy, ktorým sa nahrádza stará smernica o ePrivacy. Cieľom by bola naďalej ochrana „základných práv a slobôd fyzických a právnických osôb pri poskytovaní a využívaní elektronických komunikačných služieb, a to predovšetkým práva na rešpektovanie súkromného života a komunikácií a ochranu fyzických osôb v oblasti spracovania osobných údajov.“ Novým návrhom sa zároveň zabezpečuje voľný pohyb údajov v elektronických komunikáciách a elektronických komunikačných službách rámci Únie⁹²⁴. Zatiaľ čo všeobecné nariadenie o ochrane údajov sa v prvom rade zaoberá článkom 8

920 Pozri zmenenú smernicu, článok 13.

921 Pozri tamže, článok 5; pozri tiež dokument pracovnej skupiny zriadenej podľa článku 29 (2012), *Stanovisko 4/2012 k vyňatiu z povinnosti získať súhlas s cookies*, WP 194, Brusel, 7. júna 2012.

922 Pozri aj dokument pracovnej skupiny zriadenej podľa článku 29 (2011), *Pracovný dokument 01/2011 o súčasnom rámci EÚ pre porušenie ochrany osobných údajov a odporúčania pre budúci politický vývoj*, WP 184, Brusel, 5. apríla 2011.

923 Smernica Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES, Ú. v. EÚ L 105, 2006.

924 Návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (nariadenie o súkromí a elektronických komunikáciách), COM(2017) 10 final, článok 1.

Charty, cieľom navrhovaného nariadenia je začleniť článok 7 Charty do sekundárneho práva EÚ.

Nariadením by sa prispôbili ustanovenia predchádzajúcej smernice novým technológiám a realite na trhu a vytvoril by sa komplexný a konzistentný rámec spolu so všeobecným nariadením o ochrane údajov. V tomto zmysle by nariadenie o súkromí a elektronických komunikáciách predstavovalo *lex specialis* vo vzťahu k všeobecnému nariadeniu o ochrane údajov, prispôbovalo by ho údajom v elektronických komunikáciách, ktoré sa považujú za osobné údaje. Nové nariadenie sa vzťahuje na spracúvanie „údajov v elektronických komunikáciách“ vrátane obsahu elektronických komunikácií a metaúdajov, ktoré nie sú nevyhnutne osobnými údajmi. Územná pôsobnosť je obmedzená na EÚ, a to aj vtedy, keď sa údaje získané v EÚ spracúvajú mimo nej, a rozširuje sa na poskytovateľov komunikačných over-the-top služieb. Ide o poskytovateľov služieb, ktorí poskytujú obsah, služby alebo aplikácie cez internet bez priameho zapojenia prevádzkovateľa siete alebo poskytovateľa internetových služieb. K takýmto poskytovateľom patrí napríklad Skype (hlasové volania a videohovory), WhatsApp (posielanie správ), Google (vyhľadávanie), Spotify (hudba) alebo Netflix (video). Mechanizmy presadzovania všeobecného nariadenia o ochrane údajov by sa uplatňovali aj na nové nariadenie.

Nariadenie o súkromí a elektronických komunikáciách má byť prijaté pred 25. májom 2018, pričom do tohto dátumu bude všeobecné nariadenie o ochrane údajov uplatniteľné vo všetkých 28 členských štátoch. Je to však podmienené súhlasom Európskeho parlamentu a Rady⁹²⁵.

9.2. Údaje o zamestnaní

Hlavné body

- Osobitné pravidlá pre ochranu údajov o pracovnoprávných vzťahoch sú uvedené v odporúčaní Rady Európy o údajoch o zamestnaní.
- Vo všeobecnom nariadení o ochrane údajov sa pracovnoprávne vzťahy osobitne uvádzajú len v súvislosti so spracúvaním citlivých údajov.

⁹²⁵ Pre viac informácií pozri Európska komisia (2017), „Komisia navrhuje prísne pravidlá ochrany súkromia a údajov vo všetkých spôsoboch elektronickej komunikácie a aktualizuje pravidlá ochrany údajov v inštitúciách EÚ“, tlačová správa, 10. januára 2017.

- Platnosť súhlasu, ktorý musí byť poskytnutý slobodne, ako právneho základu pre spracúvanie údajov o zamestnancoch je možné spochybniť vzhľadom na hospodársku nerovnováhu medzi zamestnávateľom a zamestnancami. Musia sa dôkladne posúdiť okolnosti súhlasu.

Spracúvanie údajov v súvislosti so zamestnaním podlieha všeobecným právnym predpisom EÚ o ochrane osobných údajov. Jedno nariadenie⁹²⁶ sa však (okrem iného) osobitne zaoberá ochranou spracúvania osobných údajov európskymi inštitúciami v súvislosti so zamestnaním. Vo všeobecnom nariadení o ochrane údajov sa pracovnoprávne vzťahy výslovne uvádzajú v článku 9 ods. 2, v ktorom sa uvádza, že osobné údaje možno spracúvať pri plnení povinností alebo pri výkone osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti zamestnania.

Podľa všeobecného nariadenia o ochrane údajov by mal mať zamestnanec možnosť jasne odlíšiť údaje, pri ktorých dobrovoľne súhlasí s ich spracúvaním a uchovávaním, a účely, na ktoré sú jeho údaje uchovávané. Zamestnanci by pred udelením súhlasu mali byť informovaní aj o svojich právach a o dĺžke uchovávania údajov. Ak dôjde k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, zamestnávateľ musí toto porušenie oznámiť zamestnancovi. Podľa článku 88 tohto nariadenia sa členským štátom umožňuje stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd zamestnancov v súvislosti s ich osobnými údajmi v kontexte zamestnania.

Príklad: Vo veci *Worten*⁹²⁷ údaje zahŕňali záznam o pracovnom čase, ktorý obsahoval denný pracovný čas a doby odpočinku, čo predstavuje osobné údaje. Podľa vnútroštátnych právnych predpisov sa môže vyžadovať, aby zamestnávateľ poskytol záznamy o pracovnom čase vnútroštátnym orgánom príslušným v oblasti dohľadu nad pracovnými podmienkami. Išlo by o umožnenie okamžitého prístupu k príslušným osobným údajom. Prístup k osobným údajom je však potrebný na to, aby mohol vnútroštátny orgán vykonávať dohľad nad právnou úpravou pracovných podmienok⁹²⁸.

926 Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o volnom pohybe takýchto údajov, Ú. v. ES L 8.

927 SDEÚ, C-342/12, *Worten – Equipamentos para o Lar, SA/Autoridade para as Condições de Trabalho (ACT)*, 30. mája 2013, bod 19.

928 Tamže, bod 43.

Pokiaľ ide o **RE**, odporúčanie o údajoch o zamestnaní bolo vydané v roku 1989 a revidované v roku 2015⁹²⁹. Odporúčanie sa vzťahuje na spracúvanie osobných údajov na účely zamestnania v súkromnom aj vo verejnom sektore. Spracúvanie musí byť v súlade s určitými zásadami a obmedzeniami, ako je zásada transparentnosti a konzultácia so zástupcami zamestnancov pred tým, ako sa na pracoviskách zavedú monitorovacie systémy. V odporúčaní sa tiež uvádza, že zamestnávateľia by mali uplatňovať preventívne opatrenia, napríklad filtre, namiesto monitorovania využívania internetu zo strany zamestnancov.

Prehľad najbežnejších problémov ochrany údajov v súvislosti s pracovným pomerom možno nájsť v pracovnom dokumente pracovnej skupiny zriadenej podľa článku 29⁹³⁰. Pracovná skupina analyzovala význam súhlasu ako právneho základu na spracúvanie údajov o zamestnaní⁹³¹. Zistila, že ekonomická nerovnováha medzi zamestnávateľom, ktorý žiada o súhlas, a zamestnancom, ktorý udeľuje súhlas, často vyvoláva pochybnosti o tom, či súhlas bol poskytnutý slobodne. Okolnosti, za ktorých sa súhlas využíva ako právny základ na spracúvanie údajov, by sa preto mali starostlivo zvážiť pri posudzovaní platnosti súhlasu v kontexte zamestnania.

Bežným problémom v oblasti ochrany údajov v súčasnom bežnom pracovnom prostredí je rozsah legitímneho monitorovania elektronických komunikácií zamestnancov na pracovisku. Často sa tvrdí, že tento problém možno jednoducho vyriešiť zákazom súkromného používania služobných komunikačných prostriedkov. Takýto všeobecný zákaz by však bol neprimeraný a nereálny. V tejto súvislosti majú osobitný význam rozsudky ESLP vo veciach *Copland/Spojené kráľovstvo* a *Bărbulescu/Rumunsko*.

Príklad: Vo veci *Copland/Spojené kráľovstvo*⁹³² išlo o tajné monitorovanie používania služobného telefónu, elektronickej pošty a internetu zamestnankyňou vysokej školy s cieľom potvrdiť, či skutočne neprimerane používa služobné prostriedky na osobné účely. ESLP konštatoval, že telefonické hovory z pracovných priestorov patria do rozsahu pojmov súkromný život a korešpondencia. Preto sú takéto hovory a e-maily zaslané zo zamestnania,

929 Rada Európy, Výbor ministrov (2015), Odporúčanie Rec (2015) 5 členským štátom o spracúvaní osobných údajov v súvislosti so zamestnaním, apríl 2015.

930 Pracovná skupina zriadená podľa článku 29 (2017), *Stanovisko č. 2/2017 k spracúvaniu údajov v práci*, WP 249, Brusel, 8. júna 2017.

931 Pracovná skupina zriadená podľa článku 29 (2005), *Pracovný dokument o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995*, WP 114, Brusel, 25. novembra 2005.

932 ESLP, *Copland/Spojené kráľovstvo*, č. 62617/00, 3. apríla 2007.

ako aj informácie získané na základe monitorovania súkromného využívania internetu chránené článkom 8 ECHR. V prípade sťažovateľky neexistovali žiadne ustanovenia, ktorými by sa upravovali podmienky, za ktorých by zamestnávateľia mohli monitorovať používanie telefónu, e-mailu a internetu zamestnancami. Zásah teda nebol v súlade s právnymi predpismi. Súd dospel k záveru, že došlo k porušeniu článku 8 ECHR.

Príklad: Vo veci *Bărbulescu/Rumunsko*⁹³³ bol sťažovateľ prepustený za používanie internetu na pracovisku počas pracovného času v rozpore s vnútornými predpismi. Jeho zamestnávateľ monitoroval jeho komunikáciu. Počas vnútroštátneho konania boli predložené záznamy, ktoré obsahovali správy čisto súkromnej povahy. EŠLP tým, že dospel k záveru, že článok 8 je uplatniteľný, ponecháva otvorenú otázku, či reštriktívne predpisy zamestnávateľa ponechávajú žalobcovi primerané očakávanie súkromia, ale dospel k záveru, že pokyny zamestnávateľa nemôžu redukovať súkromný spoločenský život na pracovisku na nulu.

Vo veci samej bolo zmluvným štátom potrebné poskytnúť širokú mieru voľnej úvahy pri posudzovaní potreby vytvorenia právneho rámca upravujúceho podmienky, za ktorých by zamestnávateľ mohol regulovať elektronickú alebo inú komunikáciu svojich zamestnancov na pracovisku, ktorá nie je pracovnej povahy. Vnútroštátne orgány však museli zabezpečiť, aby zavedenie opatrení na monitorovanie korešpondencie a inej komunikácie zo strany zamestnávateľa, bez ohľadu na rozsah a trvanie takýchto opatrení, sprevádzali primerané a dostatočné záruky proti zneužitiu. Proporcionalita a procesné záruky na ochranu pred svojvôľou boli nevyhnutnými prvkami a EŠLP identifikoval niekoľko faktorov, ktoré boli za daných okolností relevantné. Patril k nim, okrem iného, rozsah monitorovania zo strany zamestnávateľa a stupeň narušenia súkromia zamestnanca, dôsledky pre zamestnanca a skutočnosť, či boli poskytnuté primerané záruky. Okrem toho, vnútroštátne orgány museli zabezpečiť, aby zamestnanec, ktorého komunikácia sa monitorovala, mal prístup k prostriedku nápravy pred súdnym orgánom s právomocou rozhodovať vo veci samej aspoň o tom, ako boli uvedené kritériá dodržané a či boli napadnuté opatrenia zákonné.

933 EŠLP, *Bărbulescu/Rumunsko* [VK], č. 61496/08, 5. septembra 2017, bod 121.

V tomto prípade ESLP zistil porušenie článku 8, pretože vnútroštátne orgány nezabezpečili primeranú ochranu práva sťažovateľa na rešpektovanie súkromného života a korešpondencie a v dôsledku toho sa nepodarilo dosiahnuť spravodlivú rovnováhu medzi dotknutými záujmami.

Podľa odporúčania RE o údajoch o zamestnaní by sa osobné údaje získavané na účely zamestnania mali získavať priamo od jednotlivých zamestnancov.

Osobné údaje získavané na účely prijímania zamestnancov sa musia obmedziť na informácie nevyhnutne potrebné na hodnotenie vhodnosti uchádzačov a ich kariérneho potenciálu.

V odporúčaní sa takisto konkrétne poukazuje na hodnotiace údaje týkajúce sa výkonnosti alebo možností jednotlivých zamestnancov. Hodnotiace údaje musia vychádzať zo spravodlivého a čestného hodnotenia a spôsob ich formulácie nesmie nikoho urážať. Táto požiadavka vyplýva zo zásady spravodlivého spracúvania a správnosti údajov.

Osobitný aspekt právnych predpisov o ochrane údajov z hľadiska vzťahu medzi zamestnávateľom a zamestnancom predstavuje úloha zástupcov zamestnancov. Zástupcovia zamestnancov smú získavať osobné údaje zamestnancov len do tej miery, do akej je to nevyhnutné na zastupovanie zamestnaneckých záujmov, alebo ak sú takéto údaje potrebné na plnenie povinností stanovených v kolektívnych zmluvách alebo na výkon dohľadu nad nimi.

Citlivé osobné údaje získané na účely zamestnania sa smú spracúvať len v konkrétnych prípadoch a v súlade so zárukami stanovenými vo vnútroštátnych právnych predpisoch. Zamestnávatelia sa smú pýtať zamestnancov alebo uchádzačov o zamestnanie na ich zdravotný stav alebo ich lekárske vyšetrenie len v prípade, že je to nevyhnutné. Môže ísť o: určenie vhodnosti na dané zamestnanie, splnenie požiadaviek preventívnej medicíny, zabezpečenie životne dôležitých záujmov dotknutej osoby alebo iných zamestnancov a jednotlivcov, umožnenie poskytnutia sociálnych príspevkov alebo odpoveď na požiadavku súdu. Údaje týkajúce sa zdravia sa nesmú získavať z iných zdrojov, ako je dotknutý zamestnanec, okrem prípadov získania výslovného a informovaného súhlasu alebo ak sa to stanovuje vnútroštátnymi právными predpismi.

Podľa odporúčania o údajoch o zamestnaní by zamestnanci mali byť informovaní o účele spracúvania ich osobných údajov, kategórii zbieraných osobných údajov, subjektoch, ktorým sa ich údaje pravidelne oznamujú, ako aj o účele a právnom základe takéhoto poskytnutia. Prístup k elektronickej komunikácii je z bezpečnostných dôvodov alebo iných legitímnych dôvodov možný len na pracovisku a takýto prístup je povolený len po tom, ako boli zamestnanci informovaní o tom, že zamestnávateľ môže k tomuto druhu komunikácie mať prístup.

Zamestnanci musia mať právo na prístup k svojim údajom o zamestnaní, ako aj právo na opravu alebo vymazanie týchto údajov. Ak sa spracúvajú hodnotiace údaje, zamestnanci musia mať právo napadnúť hodnotenie. Uvedené práva však môžu byť dočasne obmedzené na účely interného vyšetrovania. V prípade zamietnutia prístupu zamestnanca k jeho osobným údajom o zamestnaní alebo zamietnutia opravy či vymazania týchto údajov sa vo vnútroštátnych právnych predpisoch musia stanoviť vhodné postupy umožňujúce napadnutie takéhoto zamietnutia.

9.3. Údaje týkajúce sa zdravia

Hlavný bod

- Zdravotné údaje sú citlivé údaje, a preto si vyžadujú osobitnú ochranu.

Osobné údaje týkajúce sa zdravotného stavu dotknutej osoby sa kvalifikujú ako citlivé údaje podľa článku 9 ods. 1 všeobecného nariadenia o ochrane údajov a článku 6 modernizovaného Dohovoru č. 108. Vztahuje sa na ne teda prísnejší režim spracúvania údajov ako na údaje, ktoré nie sú citlivé. Vo všeobecnom nariadení o ochrane údajov sa zakazuje spracúvanie „osobných údajov týkajúcich sa zdravia“ (chápané ako „všetky údaje týkajúce sa zdravotného stavu dotknutej osoby, ktoré poskytujú informácie o minulom, súčasnom alebo budúcom fyzickom alebo duševnom zdravotnom stave dotknutej osoby“)⁹³⁴, ako aj genetických údajov a biometrických údajov, pokiaľ nie je povolené podľa článku 9 ods. 2. Oba typy údajov boli doplnené do zoznamu „osobitných kategórií údajov“⁹³⁵.

934 Všeobecné nariadenie o ochrane údajov, odôvodnenie 35.

935 Tamže, článok 2.

Príklad: Vo veci *Z./Fínsko*⁹³⁶ bývalý manžel sťažovateľky, ktorý bol infikovaný vírusom HIV, spáchal viacero sexuálnych trestných činov. Následne bol obvinený z neúmyselného zabitia na základe toho, že vedome vystavil svoje obete riziku nákazy vírusom HIV. Vnútroštátny súd nariadil, aby celý rozsudok a dokumentácia prípadu boli označené ako dôverné v lehote 10 rokov, a to napriek žiadostiam sťažovateľky o predĺženie tejto lehoty. Odvolací súd zamietol žiadosti o predĺženie a v rozsudku uviedol celé meno sťažovateľky a jej bývalého manžela. ESĽP dospel k záveru, že zásah nebol nevyhnutný v demokratickej spoločnosti, keďže ochrana zdravotných údajov má mimoriadny význam pre vykonávanie práva na rešpektovanie súkromného a rodinného života, predovšetkým, pokiaľ ide o informácie o nákaze vírusom HIV, a to vzhľadom na stigma, ktorá v mnohých spoločnostiach súvisí s týmto ochorením. Súd preto dospel k záveru, že umožniť prístup k totožnosti sťažovateľky a zdravotnému stavu, ako bol opísaný v rozsudku odvolacieho súdu, po uplynutí lehoty len 10 rokov od vynesenia rozsudku, by znamenalo porušenie článku 8 ECHR.

Podľa **právnych predpisov EÚ** sa v článku 9 ods. 2 písm. h) všeobecného nariadenia o ochrane údajov umožňuje spracúvanie zdravotných údajov na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej starostlivosti alebo liečby, alebo riadenia systémov a služieb zdravotnej starostlivosti. Spracúvanie je však prípustné len vtedy, ak ho vykonáva zdravotnícky pracovník, na ktorého sa vzťahuje povinnosť služobného tajomstva, alebo iná osoba, na ktorú sa vzťahuje rovnocenná povinnosť.

V **právnych predpisoch RE**, konkrétne v odporúčaní o zdravotných údajoch z roku 1997, sa podrobnejšie uplatňujú zásady Dohovoru č. 108 na spracúvanie údajov v oblasti zdravotníctva⁹³⁷. Navrhnuté pravidlá sú v súlade s pravidlami všeobecného nariadenia o ochrane údajov, pokiaľ ide o legitímne účely spracúvania zdravotných údajov, nevyhnutné povinnosti služobného tajomstva osôb používajúcich údaje týkajúce sa zdravia a práva dotknutých osôb týkajúce sa transparentnosti, prístupu, opravy a výmazu. Okrem toho sa zdravotné údaje, ktoré zákonne spracúvajú zdravotnícki pracovníci, nesmú prenášať orgánom presadzovania práva, okrem prípadov,

936 ESĽP, *Z./Fínsko*, č. 22009/93, 25. februára 1997, body 94 a 112; pozri tiež ESĽP, *M.S./Švédsko*, č. 20837/92, 27. augusta 1997; ESĽP, *L.L./Francúzsko*, č. 7508/02, 10. októbra 2006; ESĽP, *I./Fínsko*, č. 20511/03, 17. júla 2008; ESĽP, *K.H. a i./Slovensko*, č. 32881/04, 28. apríla 2009; ESĽP, *Szuluk/Spojené kráľovstvo*, č. 36936/05, 2. júna 2009.

937 Rada Európy, Výbor ministrov (1997), *Odporúčanie členským štátom Rec(97)5 o ochrane zdravotných údajov*, 13. februára 1997. Je potrebné uviesť, že toto odporúčanie prechádza revíziou.

keď sú poskytnuté „dostatočné záruky brániace zverejneniu, ktoré by nebolo zlučiteľné s rešpektovaním [...] súkromného života zaručeným článkom 8 ECHR“⁹³⁸. Vnútroštátne právne predpisy musia byť tiež „formulované dostatočne presne a musia poskytovať dostatočnú právnu ochranu pred svojvoľnosťou“⁹³⁹.

Odporúčanie o zdravotných údajoch tiež obsahuje osobitné ustanovenia o zdravotných údajoch nenarodených detí a právne nespôsobilých osôb, ako aj o spracúvaní genetických údajov. Výslovne sa v ňom uznáva, že vedecký výskum je dôvodom na uchovávanie údajov dlhšie, než sú potrebné, aj keď zvyčajne sa v takom prípade vyžaduje anonymizácia. Podrobnejšie predpisy pre situácie, v ktorých výskumníci potrebujú osobné údaje a nestačia im anonymné údaje, obsahuje článok 12 odporúčania o zdravotných údajoch.

Vhodným spôsobom uspokojenia vedeckých potrieb a súčasného zaistenia ochrany záujmov dotknutých pacientov môže byť pseudonymizácia. Konceptia pseudonymizácie v kontexte ochrany údajov je podrobnejšie vysvetlená v [oddiele 2.1.1](#).

Odporúčanie RE z roku 2016 o údajoch vyplývajúcich z genetických testov sa vzťahuje aj na spracúvanie údajov v oblasti medicíny⁹⁴⁰. Toto odporúčanie má veľký význam pre oblasť elektronického zdravotníctva (eHealth), kde sa IKT využívajú na uľahčenie lekárskej starostlivosti. Príkladom je zaslanie výsledkov rodičovského testu pacienta medzi poskytovateľmi zdravotnej starostlivosti. Cieľom tohto odporúčania je chrániť práva osôb, ktorých osobné údaje sa spracúvajú na účely poistenia proti rizikám súvisiacim so zdravím, fyzickou integritou, vekom alebo smrťou osoby. Poistovatelia musia odôvodniť spracúvanie údajov súvisiacich so zdravím, ktoré by malo byť primerané povahe a významu posudzovaného rizika. Spracúvanie tohto druhu údajov závisí od súhlasu dotknutej osoby. Poistovatelia by mali mať zavedené aj záruky pre prípady uchovávaní údajov súvisiacich so zdravím.

Klinické skúšanie liekov, ktoré zahŕňa posúdenie účinkov nových liekov na pacientov v dokumentovanom výskumnom prostredí, má značné dôsledky v oblasti ochrany údajov. Klinické skúšanie liekov na humánne použitie sa upravuje nariadením Európskeho parlamentu a Rady (EÚ) č. 536/2014 zo 16. apríla 2014 o klinickom skúšaní

938 ESĽP, *Avilkina a i./Rusko*, č. 1585/09, 6. júna 2013, bod 53. Pozri tiež ESĽP, *Biriuk/Litva*, č. 23373/03, 25. novembra 2008.

939 ESĽP, *L.H./Lotyšsko*, č. 52019/07, 29. apríla 2014, bod 59.

940 Rada Európy, Výbor ministrov (2016), Odporúčanie Rec(2016)8 členským štátom o spracúvaní osobných zdravotných údajov na účely poistenia vrátane údajov vyplývajúcich z genetických testov, 26. októbra 2016.

liekov na humánne použitie, ktorým sa zrušuje smernica 2001/20/ES (nariadenie o klinickom skúšaní liekov)⁹⁴¹. Hlavnými prvkami nariadenia o klinickom skúšaní liekov sú:

- zjednodušené podávanie žiadostí prostredníctvom portálu EÚ⁹⁴²,
- lehoty na posúdenie žiadosti o klinické skúšanie⁹⁴³,
- etická komisia, ktorá je súčasťou posudzovania, v súlade s právom členských štátov (a s európskym právom vymedzujúcim príslušné lehoty)⁹⁴⁴ a
- zlepšenie transparentnosti klinického skúšania a jeho výsledkov⁹⁴⁵.

Vo všeobecnom nariadení o ochrane údajov sa uvádza, že na účely súhlasu s účasťou na činnostiach vedeckého výskumu v klinickom skúšaní sa uplatňuje nariadenie (EÚ) č. 536/2014⁹⁴⁶.

Na úrovni EÚ prebiehajú mnohé ďalšie legislatívne a iné iniciatívy týkajúce sa osobných údajov v sektore zdravotníctva⁹⁴⁷.

Elektronické zdravotné záznamy

Elektronický zdravotný záznam je „komplexný lekársky záznam alebo podobný dokument o minulom a prítomnom fyzickom a duševnom zdravotnom stave jednotlivca v elektronickej forme, ktorý umožňuje okamžitú dostupnosť týchto údajov na účely lekárskeho ošetrovania a na iné účely s tým úzko súvisiace“⁹⁴⁸. Elektronické zdravotné záznamy sú elektronické verzie záznamov o anamnéze pacientov a môžu

941 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 536/2014 zo 16. apríla 2014 o klinickom skúšaní liekov na humánne použitie, ktorým sa zrušuje smernica 2001/20/ES (nariadenie o klinickom skúšaní liekov), Ú. v. EÚ L 158.

942 Nariadenie o klinickom skúšaní liekov, článok 5 ods. 1.

943 Tamže, článok 5 ods. 2 – 5.

944 Tamže, článok 2 ods. 2 bod 11.

945 Tamže, článok 9 ods. 1 a odôvodnenie 67.

946 Všeobecné nariadenie o ochrane údajov, odôvodnenia 156 a 161.

947 EDPS (2013), *Stanovisko Európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie s názvom Akčný plán elektronického zdravotníctva na roky 2012 – 2020 – inováčná zdravotná starostlivosť pre 21. storočie*, Brusel, 27. marca 2013.

948 *Odporúčanie Komisie z 2. júla 2008 o cezhraničnej interoperabilite systémov elektronických zdravotných záznamov*, bod 3 písm. c)

zahŕňať klinické údaje týkajúce sa týchto osôb, ako je anamnéza v minulosti, problémy a ochorenia, lieky a liečba, ako aj výsledky prehliadok a laboratórnych testov a správ. Prístup k týmto elektronickým súborom, pri ktorých môže ísť od kompletných záznamov až po jednoduché výpisy alebo zhrnutia, môže mať všeobecný lekár, lekárnik a iní zdravotnícki pracovníci. Pojem „elektronického zdravotníctva“ (eHealth) sa týka aj týchto zdravotných záznamov.

Príklad: Pán A uzavrel poisťnú zmluvu so spoločnosťou B, ktorá je poisťovateľom. Poisťovateľ bude od pána A získavať niektoré informácie týkajúce sa zdravia, ako sú pretrvávajúce zdravotné problémy alebo ochorenia. Poisťovateľ by mal uchovávať osobné údaje pána A oddelene od iných údajov. Poisťovateľ musí takisto uchovávať osobné údaje súvisiace so zdravím oddelene od iných osobných údajov. To znamená, že iba osoba zodpovedná za prípad pána A bude mať prístup k jeho zdravotným údajom.

Niektoré otázky týkajúce sa ochrany údajov však vznikajú v súvislosti s elektronickými zdravotnými záznamami, napríklad pokiaľ ide o ich dostupnosť, riadne uchovávanie a prístup k nim dotknutou osobou.

Okrem elektronických zdravotných záznamov uverejnila Európska komisia 10. apríla 2014 Zelenú knihu o mobilnom zdravotníctve (mHealth), v ktorej sa uvádza, že mobilné zdravotníctvo je novovznikajúcou a rozvíjajúcou sa oblasťou, ktorá má potenciál transformovať zdravotnú starostlivosť a zvýšiť jej efektívnosť a kvalitu. Tento pojem zahŕňa lekársku prax a poskytovanie služieb v oblasti verejného zdravia s podporou mobilných zariadení, ako sú mobilné telefóny, zariadenia na monitorovanie pacientov, osobné digitálne pomôcky a iné bezdrôtové zariadenia, ako aj aplikácie (napríklad aplikácie na zabezpečenie telesnej a duševnej pohody), ktoré sa môžu pripojiť k zdravotníckym pomôckam alebo snímačom⁹⁴⁹. V dokumente sa uvádzajú riziká pre právo na ochranu osobných údajov, ktoré by rozvoj mobilného zdravotníctva (mHealth) so sebou mohol priniesť, a uvádza, že vzhľadom na citlivú povahu údajov týkajúcich sa zdravia by mal vývoj zahŕňať konkrétne a primerané bezpečnostné záruky, ako je šifrovanie údajov o pacientovi a vhodné mechanizmy identifikácie pacientov, s cieľom zmierniť bezpečnostné riziká. Dodržiavanie pravidiel ochrany osobných údajov vrátane povinnosti poskytovať informácie dotknutej osobe, bezpečnosť údajov a uplatňovanie zásady zákonného spracúvania osobných

⁹⁴⁹ Európska komisia (2014), *Zelená kniha o mobilnom zdravotníctve (mHealth)*, COM (2014) 219 final, Brusel, 10. apríla 2014.

údajov je preto dôležité na budovanie dôvery v riešenia mobilného zdravotníctva (mHealth)⁹⁵⁰. Na tento účel sa v odvetví pripravuje kódex správania, vychádzajúci z informácií od širokej škály zainteresovaných strán vrátane zástupcov s odbornými znalosťami v oblasti ochrany údajov, samoregulácie a spoluregulácie, IKT a zdravotnej starostlivosti⁹⁵¹. V čase prípravy tejto príručky bol návrh kódexu správania predložený na pripomienkovanie pracovnej skupine pre ochranu údajov zriadenej podľa článku 29 a čakalo sa na jeho formálne schválenie.

9.4. Spracúvanie údajov na výskumné a štatistické účely

Hlavné body

- Údaje získané na štatistické účely alebo na účely vedeckého alebo historického výskumu sa nesmú použiť na žiadny iný účel.
- Údaje legítimne získané na akýkoľvek účel sa môžu ďalej použiť na štatistické účely alebo na účely vedeckého alebo historického výskumu pod podmienkou, že sa zavedú primerané záruky. Na tento účel môže záruky poskytnúť anonymizácia alebo pseudonymizácia údajov pred poskytnutím tretím stranám.

Podľa **právnych predpisov** EÚ sa umožňuje spracúvanie údajov na štatistické účely a na účely vedeckého alebo historického výskumu za predpokladu, že existujú primerané záruky pre práva a slobody dotknutých osôb. Tie môžu zahŕňať pseudonymizáciu⁹⁵². V práve EÚ alebo vo vnútroštátnom práve sa môžu stanoviť určité výnimky z práv dotknutých osôb, ak takéto práva pravdepodobne znemožnia alebo závažným spôsobom sťažia dosiahnutie legítimného účelu výskumu⁹⁵³. Môžu sa zaviesť výnimky z práva na prístup dotknutej osoby, práva na opravu, práva na obmedzenie spracúvania a práva namietat.

Hoci údaje, ktoré prevádzkovateľ zákonne získal na akýkoľvek účel, môže prevádzkovateľ opäť použiť na vlastné štatistické účely, účely vedeckého alebo historického výskumu, údaje sa musia anonymizovať alebo prípadne pseudonymizovať,

⁹⁵⁰ Tamže, s. 8.

⁹⁵¹ Návrh kódexu správania pre mobilné zdravotnícke aplikácie z hľadiska súkromia, 7. júna 2016.

⁹⁵² Všeobecné nariadenie o ochrane údajov, článok 89 ods. 1.

⁹⁵³ Tamže, článok 89 ods. 2.

v závislosti od kontextu, pred ich poskytnutím tretej strane na štatistické účely, účely vedeckého alebo historického výskumu, s výnimkou prípadu, keď dotknutá osoba poskytla súhlas alebo sa to osobitne stanovuje vo vnútroštátnom práve. Pseudonymizované údaje naďalej podliehajú všeobecnému nariadeniu o ochrane údajov, na rozdiel od anonymných údajov⁹⁵⁴.

V tomto nariadení sa osobitne upravuje oblasť výskumu, pokiaľ ide o všeobecné pravidlá ochrany údajov, s cieľom vyhnúť sa obmedzeniam v oblasti rozvoja výskumu a dosiahnuť vytvorenie európskeho výskumného priestoru, ako sa uvádza v článku 179 ZFEÚ. Týmto článkom sa zabezpečuje široký výklad spracúvania osobných údajov na účely vedeckého výskumu, aby zahŕňalo technický rozvoj a demonštračné činnosti, základný výskum, aplikovaný výskum a výskum financovaný zo súkromných zdrojov. Uznáva sa aj význam zhromažďovania údajov v registroch na výskumné účely a možné ťažkosti pri úplnom určovaní následného účelu spracúvania osobných údajov na účely vedeckého výskumu v čase získavania údajov⁹⁵⁵. Z tohto dôvodu sa nariadením umožňuje spracúvanie údajov na tieto účely bez súhlasu dotknutých osôb za predpokladu, že sú zavedené príslušné záruky.

Dôležitým príkladom využívania údajov na štatistické účely sú oficiálne štatistiky získané národnými štatistickými úradmi a štatistickými úradmi EÚ podľa vnútroštátnych právnych predpisov a právnych predpisov EÚ o oficiálnych štatistikách. Podľa týchto predpisov sú občania a podniky zvyčajne povinní poskytovať údaje príslušným štatistickým úradom. Úradníci, ktorí pracujú na štatistických úradoch, sú viazaní osobitnou povinnosťou zachovávať služobné tajomstvo, ktorá sa musí riadne dodržiavať, pretože je to nevyhnutné na zabezpečenie vysokej úrovne dôvery občanov potrebnej na poskytovanie údajov štatistickým orgánom⁹⁵⁶.

Základné pravidlá týkajúce sa ochrany údajov v oficiálnych štatistikách obsahuje nariadenie (ES) č. 223/2009 o európskej štatistike (nariadenie o európskej štatistike), a môže sa teda pokladať za relevantné pre ustanovenia o oficiálnych štatistikách na

954 Tamže, odôvodnenie 26.

955 Tamže, odôvodnenia 33, 157 a 159.

956 Tamže, článok 90.

vnútroštátnej úrovni⁹⁵⁷. Nariadením sa presadzuje zásada, podľa ktorej oficiálne štatistické operácie potrebujú dostatočne jasný právny základ⁹⁵⁸.

Príklad: Vo veci *Huber/Bundesrepublik Deutschland*⁹⁵⁹ sa pán Huber, rakúsky podnikateľ, ktorý sa presťahoval do Nemecka, sťažoval, že získavaním a uchovávaním osobných údajov cudzích štátnych príslušníkov, ktoré vykonávali nemecké orgány v centrálnom registri (AZR) aj na štatistické účely, sa porušujú jeho práva podľa smernice o ochrane údajov. Vzhľadom na to, že cieľom smernice 95/46 je zabezpečiť rovnocennú úroveň ochrany údajov vo všetkých členských štátoch, SDEÚ rozhodol, že na zabezpečenie vysokej úrovne ochrany v EÚ pojem nevyhnutnosti podľa článku 7 písm. e) nemôže mať v jednotlivých členských štátoch odlišný význam. Ide teda o pojem, ktorý má v práve Únie samostatný význam a musí sa vykladať spôsobom, ktorý plne zodpovedá cieľu smernice 95/46. SDEÚ konštatoval, že na štatistické účely by sa mali vyžadovať len anonymné informácie, a rozhodol, že nemecký register nie je v súlade s požiadavkou nevyhnutnosti podľa článku 7 písm. e).

V kontexte **RE** sa môže ďalšie spracúvanie údajov vykonávať na vedecké, historické alebo štatistické účely, ak je to vo verejnom záujme, a musí podliehať primeraným zárukám⁹⁶⁰. Práva dotknutých osôb sa môžu obmedziť aj pri spracúvaní údajov na štatistické účely za predpokladu, že neexistuje žiadne rozpoznateľné riziko porušenia ich práv a slobôd⁹⁶¹.

957 Nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 z 11. marca 2009 o európskej štatistike a o zrušení nariadenia (ES, Euratom) č. 1101/2008 o prenose dôverných štatistických údajov Štatistickému úradu Európskych spoločenstiev, nariadenia Rady (ES) č. 322/97 o štatistike Spoločenstva a rozhodnutia Rady 89/382/EHS, Euratom o založení Výboru pre štatistické programy Európskych spoločenstiev, Ú. v. EÚ L 87, 2009, zmenené nariadením Európskeho parlamentu a Rady (EÚ) 2015/759 z 29. apríla 2015, ktorým sa mení nariadenie (ES) č. 223/2009 o európskej štatistike, Ú. v. EÚ L 123, 2015.

958 Táto zásada sa podrobnejšie opisuje v *Kódexe postupov Eurostatu*, ktorý v súlade s článkom 11 nariadenia o európskej štatistike poskytuje etické usmernenia k príprave oficiálnych štatistik vrátane opatreného používania osobných údajov.

959 SDEÚ, C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008, pozri najmä bod 68.

960 Modernizovaný Dohovor č. 108, článok 5 ods. 4 písm. b).

961 Tamže, článok 11 ods. 2.

Odporúčanie o štatistických údajoch vydané v roku 1997 sa vzťahuje na vykonávanie štatistickej činnosti vo verejnom a súkromnom sektore⁹⁶².

Údaje získané prevádzkovateľom na štatistické účely sa nesmú použiť na žiadny iný účel. Údaje získané na iné ako štatistické účely je možné použiť aj na štatistické účely. V odporúčaní o štatistických údajoch sa umožňuje aj oznamovanie údajov tretím stranám za predpokladu, že je to len na štatistické účely. V takýchto prípadoch by sa strany mali dohodnúť a písomne stanoviť rozsah ďalšieho legitímneho použitia na štatistické účely. Keďže sa tým nemôže nahradiť súhlas dotknutej osoby – v prípade potreby –, musia byť vo vnútroštátnom práve stanovené primerané záruky, aby sa minimalizovali riziká zneužitia osobných údajov, napríklad povinnosť anonymizovať alebo pseudonymizovať údaje pred ich poskytnutím.

Odborníci v oblasti štatistického výskumu musia byť podľa vnútroštátnych právnych predpisov viazaní osobitnou povinnosťou zachovávať služobné tajomstvo, ako je to zvyčajne v prípade oficiálnych štatistik. Táto povinnosť sa musí rozšíriť aj na anketárov a iné subjekty, ktoré získavajú osobné údaje, ak sa využijú pri získavaní údajov od dotknutých osôb alebo iných osôb.

Ak štatistický prieskum, pri ktorom sa využívajú osobné údaje, nie je povolený podľa zákona, jeho legitímnosť je potrebné zabezpečiť získaním súhlasu dotknutých osôb s použitím ich údajov, alebo tým, že sa im poskytne možnosť namietat'. Ak osobné údaje získavajú anketári na štatistické účely, opýtaní musia byť jasne informovaní o tom, či je poskytnutie údajov podľa vnútroštátneho práva povinné.

Ak nie je možné uskutočniť štatistický prieskum s anonymnými údajmi a musia sa použiť osobné údaje, mali by sa údaje získané na tento účel čo najskôr anonymizovať. Výsledky štatistického prieskumu minimálne nesmú umožňovať identifikáciu žiadnej dotknutej osoby, okrem prípadov, keď by identifikácia preukázateľne neznamenalala žiadne riziko.

Po ukončení štatistickej analýzy by sa osobné údaje mali buď vymazať, alebo anonymizovať. V odporúčaní o štatistických údajoch sa v tomto prípade navrhuje uchovávať identifikačné údaje oddelene od ostatných osobných údajov. To znamená, že napríklad buď šifrovací kľúč, alebo zoznam identifikačných synonym by sa mali uchovávať oddelene od ostatných údajov.

⁹⁶² Rada Európy, Výbor ministrov (1997), Odporúčanie členským štátom Rec(97)18 o ochrane osobných údajov zbieraných a spracúvaných na štatistické účely, 30. septembra 1997.

9.5. Finančné údaje

Hlavné body

- Aj keď finančné údaje nie sú citlivými údajmi v zmysle modernizovaného Dohovoru č. 108 alebo všeobecného nariadenia o ochrane údajov, ich spracúvanie si vyžaduje osobitné záruky na zaistenie správnosti a bezpečnosti údajov.
- Do elektronických platobných systémov musí byť zabudovaná ochrana údajov, tzv. špecificky navrhnutá a štandardná ochrana súkromia alebo údajov.
- Konkrétne problémy týkajúce sa ochrany údajov v tejto oblasti vznikajú v súvislosti s potrebou zaviesť vhodné mechanizmy autentifikácie.

Príklad: Vo veci *Michaud/Francúzsko*⁹⁶³ sťažovateľ (francúzsky právnik) spochybnil povinnosť hlásiť podozrenia týkajúce sa možného prania špinavých peňazí zo strany klientov, ktorá je stanovená vo francúzskych právnych predpisoch. ESLP konštatoval, že povinnosť právnikov, aby orgánom štátnej správy poskytovali informácie o inej osobe, ku ktorým získajú prístup na základe ich profesijného spojenia sa s danou osobou, predstavuje zasahovanie do práva právnikov na rešpektovanie ich korešpondencie a súkromného života podľa článku 8 ECHR, keďže tento pojem zahŕňa činnosti profesijnej a obchodnej povahy. Dané zasahovanie však bolo v súlade s právnymi predpismi a sledovalo legitímny cieľ, a to predchádzanie narušeniu verejného poriadku a trestnej činnosti. Keďže právnici boli povinní hlásiť podozrenie len za veľmi špecifických okolností, ESLP konštatoval, že táto povinnosť je primeraná. ESLP dospel k záveru, že nedošlo k porušeniu článku 8.

Príklad: Vo veci *M.N. a i./San Marino*⁹⁶⁴ sťažovateľ, taliansky občan, uzavrel fiduciárnu dohodu so spoločnosťou, ktorá bola predmetom vyšetrovania. To znamená, že v spoločnosti došlo k prehliadke a zaisteniu kópií (elektronickej) dokumentácie. Sťažovateľ podal sťažnosť na súd v San Marine, pričom tvrdil, že medzi ním a údajnými trestnými činmi neexistuje žiadna súvislosť. Súd však vyhlásil jeho sťažnosť za neprípustnú, keďže nebol „zúčastnenou stranou“. ESLP rozhodol, že sťažovateľ bol v porovnaní so „zúčastnenou stranou“

963 ESLP, *Michaud/Francúzsko*, č. 12323/11, 6. decembra 2012. Pozri tiež ESLP, *Niemietz/Nemecko*, č. 13710/88, 16. decembra 1992, bod 29, a ESLP, *Halford/Spojené kráľovstvo*, č. 20605/92, 25. júna 1997, bod 42.

964 ESLP, *M.N. a i./San Marino*, č. 28005/12, 7. júla 2015.

značne znevýhodnený, pokiaľ ide o možnosti súdnej ochrany, jeho údaje však napriek tomu boli predmetom prehliadky a zaistenia. Súd teda rozhodol, že došlo k porušeniu článku 8.

Príklad: Vo veci *G.S.B./Švajčiarsko*⁹⁶⁵ boli údaje o bankovom účte sťažovateľa zaslané daňovým orgánom Spojených štátov na základe dohody o administratívnej spolupráci medzi Švajčiarskom a USA. ESLP konštatoval, že poskytnutie nebolo v rozpore s článkom 8 ECHR, pretože zásah do práva na súkromie sťažovateľa bol v súlade so zákonom, sledoval legitímny cieľ a bol primeraný sledovanému verejnému záujmu.

Uplatňovaním všeobecného právneho rámca ochrany údajov (stanoveného Dohovorom č. 108) sa v kontexte platieb zaoberala **RE** v odporúčaní Rec(90)19 z roku 1990⁹⁶⁶. V tomto odporúčaní sa vysvetľuje rozsah zákonného získavania a používania údajov v kontexte platieb, a to najmä prostredníctvom platobných kariet. Ďalej sa zákonodarcom v jednotlivých členských štátoch poskytujú podrobné odporúčania týkajúce sa pravidiel pri oznamovaní platobných údajov tretím stranám, časových limitov uchovávanía údajov, transparentnosti, bezpečnosti údajov a cezhraničných tokoch údajov, ako aj o dohľade a prostriedkoch nápravy. RE tiež vypracovala stanovisko o prenose daňových údajov⁹⁶⁷, v ktorom sa uvádzajú odporúčania a otázky, ktoré sa majú zohľadniť pri poskytovaní daňových údajov.

ESLP umožňuje poskytovanie finančných údajov – konkrétne údajov o bankovom účte fyzickej osoby – podľa článku 8 ECHR, ak je v súlade so zákonom, sleduje legitímny cieľ a je primeraný sledovanému verejnému záujmu⁹⁶⁸.

Pokiaľ ide o **právne predpisy EÚ**, elektronické platobné systémy, ktoré zahŕňajú spracúvanie osobných údajov, musia byť v súlade so všeobecným nariadením o ochrane údajov. Tieto systémy preto musia zabezpečiť špecificky navrhnutú a štandardnú ochranu údajov. V rámci špecificky navrhutej ochrany údajov sa ukladá prevádzkovateľovi povinnosť prijať primerané technické a organizačné opatrenia na vykonávanie zásad ochrany údajov. Štandardná ochrana údajov znamená,

965 ESLP, *G.S.B./Švajčiarsko*, č. 28601/11, 22. decembra 2015.

966 Rada Európy, Výbor ministrov (1990), Odporúčanie č. R(90)19 o ochrane osobných údajov používaných pri platbách a ďalších súvisiacich operáciách, 13. septembra 1990.

967 Rada Európy, Poradný výbor pre Dohovor č. 108 (2014), Stanovisko k vplyvu mechanizmov automatickej medzištátnej výmeny údajov na administratívne a daňové účely na ochranu údajov, 4. júna 2014.

968 ESLP, *G.S.B./Švajčiarsko*, č. 28601/11, 22. decembra 2015.

že prevádzkovateľ musí zabezpečiť, aby sa štandardne spracúvali len osobné údaje, ktoré sú potrebné na konkrétny účel (pozri [oddiel 4.4](#)). Pokiaľ ide o finančné údaje, SDEÚ konštatoval, že prenesené daňové údaje môžu predstavovať osobné údaje⁹⁶⁹. Pracovná skupina zriadená podľa článku 29 vydala súvisiace usmernenia pre členské štáty vrátane kritérií na zabezpečenie súladu s pravidlami ochrany údajov pri automatickej výmene osobných údajov na daňové účely automatizovanými prostriedkami⁹⁷⁰. Okrem toho bolo prijatých niekoľko právnych nástrojov na reguláciu finančných trhov a činností úverových inštitúcií a investičných spoločností⁹⁷¹. Ďalšie právne nástroje pomáhajú pri boji proti obchodovaniu s využitím dôverných informácií a manipulácii s trhom⁹⁷². Hlavné oblasti, ktoré majú vplyv na ochranu údajov, sú:

- uchovávanie záznamov o finančných transakciách,
- prenos osobných údajov do tretích krajín,
- nahrávanie telefonických rozhovorov alebo elektronickej komunikácie vrátane právomoci príslušných orgánov požadovať telefonické záznamy a záznamy o prevádzkových údajoch,
- sprístupnenie osobných informácií vrátane zverejnenia sankcií,
- dozorné a vyšetrovacie právomoci príslušných orgánov vrátane kontrol na mieste a vstupe do súkromných priestorov na zabavenie dokumentov,
- mechanizmy oznamovania porušení, t. j. systémy oznamovania protispoločenskej činnosti, a

969 SDEÚ, C-201/14, *Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.*, 1. októbra 2015, bod 29.

970 Pracovná skupina zriadená podľa článku 29 (2015), Vyhlásenie pracovnej skupiny zriadenej podľa článku 29 o automatickej výmene osobných údajov medzi štátmi na daňové účely, 14/EN WP 230.

971 Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ, Ú. v. EÚ L 173, 2014; nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012, Ú. v. EÚ L 173, 2014; smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES, Ú. v. EÚ L 176, 2013.

972 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 596/2014 zo 16. apríla 2014 o zneužívaní trhu (nariadenie o zneužívaní trhu) a o zrušení smernice Európskeho parlamentu a Rady 2003/6/ES a smerníc Komisie 2003/124/ES, 2003/125/ES a 2004/72/ES, Ú. v. EÚ L 173, 2014.

- spolupráca medzi príslušnými orgánmi členských štátov a Európskym orgánom pre cenné papiere a trhy (ESMA).

Osobitne sa riešia aj ďalšie problémy v týchto oblastiach vrátane získavania údajov o finančnom postavení dotknutých osôb⁹⁷³ alebo cezhraničných platbách prostredníctvom bankových prevodov, ktoré nutne vedú k vzniku tokov osobných údajov⁹⁷⁴.

973 Nariadenie Európskeho parlamentu a Rady (ES) č. 1060/2009 zo 16. septembra 2009 o ratingových agentúrach, Ú. v. EÚ L 302, 2009, a naposledy zmenené smernicou Európskeho parlamentu a Rady 2014/51/EÚ zo 16. apríla 2014, ktorou sa menia smernice 2003/71/ES a 2009/138/ES a nariadenia (ES) č. 1060/2009, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 v súvislosti s právomocami európskeho orgánu dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov) a európskeho orgánu dohľadu (Európsky orgán pre cenné papiere a trhy), Ú. v. EÚ L 153, 2014; nariadenie Európskeho parlamentu a Rady (EÚ) č. 462/2013 z 21. mája 2013, ktorým sa mení nariadenie (ES) č. 1060/2009 o ratingových agentúrach, Ú. v. EÚ L 146, 2013.

974 Smernica Európskeho parlamentu a Rady 2007/64/ES z 13. novembra 2007 o platobných službách na vnútornom trhu, ktorou sa menia a dopĺňajú smernice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a ktorou sa zrušuje smernica 97/5/ES, Ú. v. EÚ L 319, 2007, zmenená smernicou Európskeho parlamentu a Rady 2009/111/ES zo 16. septembra 2009, ktorou sa menia a dopĺňajú smernice 2006/48/ES, 2006/49/ES a 2007/64/ES, pokiaľ ide o banky pridružené k ústredným inštitúciám, niektoré položky vlastných zdrojov, veľkú majetkovú angažovanosť, mechanizmy dohľadu a krízové riadenie, Ú. v. EÚ L 302, 2009.

10

Moderné výzvy v oblasti ochrany osobných údajov

Pre tento digitálny vek alebo vek informačných technológií je charakteristické rozsiahle používanie počítačov, internetu a digitálnych technológií. Patri k tomu aj získavanie a spracúvanie obrovského množstva údajov vrátane osobných údajov. Získavanie a spracúvanie osobných údajov v globalizovanom hospodárstve znamená, že sa zvyšuje počet cezhraničných tokov údajov. Takéto spracúvanie môže pre každodenný život predstavovať významné a viditeľné výhody: vyhľadávače uľahčujú prístup k rozsiahlym objemom informácií a vedomostí, sociálne siete umožňujú ľuďom na celom svete komunikovať, vyjadrovať názory a mobilizovať podporu pre sociálne, environmentálne a politické otázky, zatiaľ čo spoločnosti a spotrebiteľia môžu využívať účinné a efektívne marketingové techniky, ktoré oživujú hospodárstvo. Technológie a spracúvanie osobných údajov sú nevyhnutnými nástrojmi aj pre štátne orgány v boji proti trestnej činnosti a terorizmu. Podobne big data – získavanie, ukladanie a analýza veľkého množstva informácií na identifikáciu vzorcov a predpovedania správania – „môžu byť zdrojom významnej hodnoty pre spoločnosť, zvyšovať produktivitu, výkonnosť vo verejnom sektore a účasť na živote spoločnosti“⁹⁷⁵.

Digitálny vek napriek mnohým výhodám so sebou prináša aj výzvy v oblasti ochrany súkromia a údajov, keďže obrovské množstvo osobných informácií sa získava a spracúva čoraz komplexnejšími a neprehľadnejšími spôsobmi. Technologický pokrok viedol k rozvoju masívnych súborov údajov, ktoré je možné jednoducho navzájom porovnávať a ďalej analyzovať s cieľom identifikovať vzorce, alebo prijímať rozhodnutia na základe algoritmov, čo môže poskytnúť nebývalý pohľad na správanie ľudí a ich súkromný život⁹⁷⁶.

975 Rada Európy, Poradný výbor pre Dohovor č. 108, *Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data*, T-PD(2017)01, Štrasburg, 23. januára 2017.

976 Európsky parlament (2017), *Uznesenie o vplyve veľkých dát na základné práva: súkromie, ochrana údajov, nediskriminácia, bezpečnosť a presadzovanie práva*, P8_TA-PROV(2017)0076, Štrasburg, 14. marca 2017.

Nové technológie sú výkonné a môžu byť obzvlášť nebezpečné, ak sa dostanú do nesprávnych rúk. Štátne orgány vykonávajúce činnosti hromadného sledovania, pri ktorých sa tieto technológie môžu využívať, sú príkladom významného vplyvu, ktorý tieto technológie môžu mať na práva jednotlivcov. Odhalenia Edwarda Snowdena z roku 2013 o existencii rozsiahlych programov spravodajských služieb zameraných na sledovanie používania internetu a telefonickej komunikácie v niektorých štátoch vyvolali značné obavy, pokiaľ ide o riziká, ktoré pri takomto sledovaní môžu ohrozovať súkromie, demokratickú správu a slobodu prejavu. Hromadné sledovanie a technológie umožňujúce globalizované uchovávanie a spracúvanie osobných informácií a hromadný prístup k údajom môžu zasahovať do samotnej podstaty práva na súkromie⁹⁷⁷. Okrem toho môžu mať negatívny vplyv na politickú kultúru a odstrašujúci účinok na demokraciu, tvorivosť a inováciu⁹⁷⁸. Už len samotné obavy, že štát môže neustále sledovať a analyzovať správanie a konanie občanov, ich môže odradiť od toho, aby vyjadrili svoje názory na určité otázky, a viesť k obozretnosti a opatrnosti⁹⁷⁹. Tieto výzvy viedli k tomu, že viacero orgánov verejnej moci, výskumných stredísk a organizácií občianskej spoločnosti začalo analyzovať potenciálne vplyvy nových technológií na spoločnosť. V roku 2015 Európsky dozorný úradník pre ochranu údajov spustil niekoľko iniciatív zameraných na posúdenie vplyvu big data a internetu vecí na etiku. Zriadil predovšetkým poradnú skupinu pre etiku, ktorej cieľom je podnietiť „otvorenú a informovanú diskusiu o digitálnej etike, ktorá umožní, aby si EÚ uvedomila výhody technológií pre spoločnosť a hospodárstvo a zároveň posilní práva a slobody jednotlivcov, najmä ich práva na súkromie a ochranu osobných údajov“⁹⁸⁰.

Spracúvanie osobných údajov je tiež silným nástrojom v rukách podnikov. V súčasnosti sa pri ňom môžu odhaliť podrobné informácie o zdravotnej alebo finančnej situácii osoby, pričom tieto informácie spoločnosti následne používajú pri prijímaní rozhodnutí dôležitých pre jednotlivcov, napríklad rozhodnutí o výške poistného na zdravotné poistenie, ktorá sa na nich má vzťahovať, alebo o ich úverovej bonite. Techniky spracúvania údajov môžu mať vplyv aj na demokratické procesy, ak ich používajú politici alebo spoločnosti na ovplyvňovanie volieb – napríklad

977 Pozri Valné zhromaždenie OSN, *Správa osobitného spravodajcu o podpore a ochrane ľudských práv a základných slobôd v boji proti terorizmu*, Ben Emmerson, A/69/397, 23. septembra 2014, bod 59. Pozri tiež ESLP, *Factsheet on Mass surveillance*, júl 2017.

978 EDPS (2015), Čeliť výzvam tzv. veľkých dát, stanovisko 7/2015, Brusel, 19. novembra 2015.

979 Pozri najmä spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i.* [VK], 8. apríla 2014, bod. 37.

980 EDPS, rozhodnutie z 3. decembra 2015, ktorým sa zriaďuje externá poradná skupina pre etické aspekty ochrany osobných údajov („poradná skupina pre etiku“), 3. decembra 2015, odôvodnenie 5.

prostredníctvom „mikrotargetingu“ komunikácie s voličmi. Inými slovami, zatiaľ čo súkromie bolo pôvodne vnímané ako právo na ochranu jednotlivcov pred neoprávneným zasahovaním orgánov verejnej moci, v súčasnosti môže byť tiež ohrozované právomocami súkromných subjektov. Vznikajú tu otázky týkajúce sa používania technológií a prediktívnej analýzy pri rozhodnutiach, ktoré ovplyvňujú každodenný život jednotlivcov, a narastá potreba zabezpečiť, aby spracúvanie osobných údajov rešpektovalo požiadavky na základné práva.

Ochrana údajov je neoddeliteľne spojená s technologickými, sociálnymi a politickými zmenami. Nebolo by preto možné zostaviť úplný zoznam budúcich výziev. Táto kapitola sa zameriava na vybrané oblasti týkajúce sa big data, internetových sociálnych sietí a digitálneho jednotného trhu EÚ. Nejde o vyčerpávajúce posúdenie týchto oblastí z hľadiska ochrany údajov, namiesto toho sa poukazuje na množstvo možných interakcií medzi novými alebo meniacimi sa ľudskými činnosťami a ochranou údajov.

10.1. Big data, algoritmy a umelá inteligencia

Hlavné body

- Disruptívne inovácie v oblasti IKT formujú nový spôsob života, v rámci ktorého sú sociálne vzťahy, obchod, súkromné a verejné služby digitálne vzájomne prepojené, pričom vzniká čoraz väčšie množstvo údajov, z ktorých mnohé sú osobnými údajmi.
- Vlády, podniky a občania čoraz viac fungujú v prostredí dátového hospodárstva, v ktorom samotné údaje majú hodnotu.
- Pojem big data sa vzťahuje na údaje, ako aj na ich analýzu.
- Na osobné údaje spracúvané v rámci analýzy big data sa vzťahujú právne predpisy EÚ a RE.
- Výnimky z pravidiel a práv v oblasti ochrany údajov sa obmedzujú na vybrané práva a na osobitné situácie, v ktorých by výkon práva nebol možný alebo by si vyžadoval neprimerané úsilie prevádzkovateľov.
- Plne automatizované rozhodovanie je vo všeobecnosti zakázané, s výnimkou osobitných prípadov.
- Informovanosť jednotlivcov a kontrola zo strany jednotlivcov sú kľúčovým prvkom pri zabezpečovaní presadzovania práv.

Vo svete, ktorý je čoraz viac digitalizovaný, každá činnosť zanecháva digitálnu stopu, ktorú možno získať, spracovať a vyhodnotiť alebo analyzovať. Vďaka novým informačným a komunikačným technológiám sa získava a zaznamenáva čoraz viac údajov⁹⁸¹. Donedávna nebola žiadna technológia schopná takéto množstvo údajov analyzovať alebo vyhodnotiť, ani vyvodzovať užitočné závery. Objem údajov bol jednoducho príliš veľký na hodnotenie, údaje boli príliš zložité, nedostatočne štruktúrované a trendy a dispozície sa rýchlo menili.

10.1.1. Vymedzenie big data, algoritmov a umelej inteligencie

Big data

Pojem „big data“ je označenie, ktoré sa môže vzťahovať na viacero koncepcií v závislosti od kontextu. Zvyčajne zahŕňa „zvyšujúcu sa technologickú schopnosť získavať, spracúvať a extrahovať nové a prediktívne poznatky z veľkého objemu, rýchlosti a rozmanitosti údajov“⁹⁸². Koncepcia big data sa preto vzťahuje tak na samotné údaje, ako aj na analýzu údajov.

Zdroje údajov sú rôzne a zahŕňajú osoby a ich osobné údaje, stroje alebo senzory, klimatické informácie, satelitné snímky, digitálne fotografie a video alebo signály z GPS. Veľké množstvo údajov a informácií však tvoria osobné údaje – akýkoľvek údaj ako je meno, fotografia, e-mailová adresa, bankové údaje, sledovacie údaje z GPS, príspevok na stránkach sociálnych sietí, zdravotné informácie alebo IP adresa počítača⁹⁸³.

Big data sa vzťahujú aj na **spracúvanie**, analýzu a vyhodnocovanie veľkých objemov údajov a dostupných informácií, t. j. na získanie užitočných informácií na účely

981 Európska komisia, oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Na ceste k prosperujúcemu hospodárstvu založenému na údajoch, COM (2014) 442 final, Brusel, 2. júla 2014.

982 Rada Európy, Poradný výbor pre Dohovor č. 108, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 2; Európska komisia, oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Na ceste k prosperujúcemu hospodárstvu založenému na údajoch, COM (2014) 442 final, Brusel, 2. júla 2014; International Telecommunications Union (2015), odporúčanie Y.3600. Big Data – Cloud computing based requirements and capabilities.

983 Informačný list Európskej komisie o reforme ochrany údajov v EÚ a Big data; Rada Európy, Poradný výbor pre Dohovor č. 108, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 2.

analýzy big data. Znamená to, že získané údaje a informácie možno použiť na iné účely než tie, na ktoré boli pôvodne určené, napr. na zisťovanie štatistických trendov alebo lepšie prispôsobenie služby, napríklad reklamy. V prípadoch, ak existujú technológie na získavanie, spracúvanie a vyhodnotenie big data, je dokonca možné kombinovať a prehodnotiť akýkoľvek druh informácie: finančné transakcie, úverová bonita, lekárske ošetrenie, súkromná spotreba, pracovná činnosť, sledovanie a používané trasy, používanie internetu, elektronické karty a smartfóny, videomonitorovanie alebo monitorovanie komunikácie. Analýza big data prináša nový kvantitatívny rozmer údajov, ktorý možno hodnotiť a používať v reálnom čase, napríklad pri poskytovaní na mieru prispôbených služieb spotrebiteľom.

Algoritmy a umelá inteligencia

Umelá inteligencia (UI) znamená inteligenciu strojov, ktoré konajú ako „inteligentné subjekty“. Ako inteligentné subjekty dokážu určité zariadenia s podporou softvéru vnímať svoje prostredie a vykonávať činnosti na základe algoritmov. Pojem umelá inteligencia sa používa v prípade, že stroj napodobňuje „kognitívne“ funkcie, ako je učenie a riešenie problémov, ktoré sa bežne pripisujú fyzickým osobám⁹⁸⁴. Pri napodobňovaní rozhodovania moderné technológie a softvér využívajú algoritmy, ktoré zariadenia používajú pri „automatizovaných rozhodnutiach“. Algoritmus je najlepšie možné opísať ako postup krokov pri výpočte, spracúvaní údajov, hodnotení a automatizovanom odôvodnení a rozhodovaní.

Podobne ako analýza big data, aj umelá inteligencia a automatizované rozhodovanie, ktoré je jej výsledkom, si vyžaduje zostavovanie a spracúvanie veľkých objemov údajov. Tieto údaje môžu pochádzať zo samotného zariadenia (teplota bŕzd, paliva atď.) alebo z okolitého prostredia. Napríklad profilovanie je proces, ktorý sa môže opierať o automatizované rozhodovanie podľa vopred stanovených vzorcov alebo faktorov.

Príklad: Profilovanie a cielená reklama

Profilovanie na základe big data si vyžaduje hľadanie vzorcov, ktoré odrážajú „charakteristiky typu osobnosti“ – napríklad, keď online predajcovia ponúkajú výrobky, „ktoré by sa vám tiež mohli páčiť“, na základe informácií získaných

984 Stuart Russel a Peter Norvig, *Artificial Intelligence: A Modern Approach* (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, s. 27, 32 – 58, 968 – 972; Stuart Russel a Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

z produktov, ktoré zákazník v minulosti vložil do nákupného košíka. Čím viac údajov, tým je mozaika jasnejšia. Napríklad smartfón je ako efektívny dotazník, ktorý jednotlivci vyplňajú pri každom jeho použití, vedome a nevedome.

Moderná psychografia – veda skúmajúca osobnosti – používa metódu OCEAN, na základe ktorej určuje typy charakterov, ktorými sa zaoberá. V rámci modelu „Big Five“ existuje päť charakteristík, otvorenosť (v akej miere je osoba otvorená novým skúsenostiam), svedomitosť (v akej miere je osoba perfekcionista), extravertzia (v akej miere je osoba spoločenská), prívetivosť (v akej miere je osoba prívetivá) a neurotizmus (v akej miere je osoba zraniteľná). Z týchto informácií vzniká profil danej osoby, jej potrieb a obáv, toho, ako sa bude správať, atď. Tento profil sa potom dopĺňa ďalšími informáciami o osobe, získanými z akýchkoľvek dostupných zdrojov, od data brokers, sociálnych sietí (vrátane kliknutí „páči sa mi“ pri zverejnených príspevkoch a fotografiách), po hudbu, ktorú počúva na internete, alebo GPS a sledovacie údaje.

Toto obrovské množstvo profilov vytvorených prostredníctvom techník analýzy big data sa následne navzájom porovnáva s cieľom identifikovať podobné vzorce a vytvoriť zoskupenia osobností. Zmení sa preto postupnosť informácií o správaní a postojoch niektorých osobností. Na základe prístupu k big data a ich používaním sa test osobnosti otočí naopak a informácie o správaní a postojoch sa použijú na opísanie osobnosti jednotlivca. Skombinovaním informácií o kliknutiach „páči sa mi“ na sociálnych sieťach, sledovacích údajoch, počúvanej hudbe alebo pozeraných filmoch možno získať jasný obraz o osobnosti jednotlivca, ktorý umožní podnikom prispôbiť cieľenú reklamu a/alebo informácie podľa „osobnosti“ tejto osoby. A navyše je tieto informácie možné spracúvať v reálnom čase⁹⁸⁵.

10.1.2. Vyvažovanie prínosov a rizík big data

Využívaním moderných techník spracúvania je možné zvládať veľké objemy údajov, rýchlo zadávať nové údaje, zabezpečiť spracúvanie informácií v reálnom čase a s krátkym reakčným časom (aj v prípade komplexných žiadostí), riešiť viacnásobné a súbežné požiadavky a analyzovať rôzne druhy informácií (fotografie, texty alebo

⁹⁸⁵ Pomocou techník spracúvania a nového softvéru sa vyhodnocujú informácie o tom, čo sa osobe páči, čo vyhľadáva pri online nakupovaní alebo pridáva do online nákupného košíka v reálnom čase, a môžu sa navrhovať „produkty“, ktoré by na základe týchto zhromaždených informácií mohli byť zaujímavé.

čísla). Tieto technologické inovácie umožňujú štruktúrovať, spracúvať a vyhodnotiť obrovské objemy údajov a informácií v reálnom čase. Exponenciálnym zvýšením množstva dostupných a analyzovaných údajov je možné získať výsledky, ktoré by pri analýze menšieho rozsahu nebolo možné získať⁹⁸⁶. Big data pomohli vytvoriť novú oblasť podnikania, v rámci ktorej môžu vznikať nové služby pre podniky aj spotrebiteľov. Hodnota osobných údajov občanov EÚ môže do roku 2020 narásť takmer na 1 bilión EUR ročne⁹⁸⁷. Pri vyhodnocovaní hromadných údajov preto big data môžu predstavovať nové **príležitosti** na nové sociálne, hospodárske alebo vedecké poznatky, z ktorých môžu profitovať jednotlivci, ako aj podniky a vlády⁹⁸⁸.

Analýza big data môže odhaliť vzorce v rôznych zdrojoch a súboroch údajov, ktoré prinášajú užitočné poznatky v oblastiach ako veda a medicína. Platí to napríklad v oblastiach ako zdravotníctvo, potravinová bezpečnosť, inteligentné dopravné systémy, energetická efektívnosť alebo územné plánovanie. Túto analýzu informácií v reálnom čase možno použiť na zlepšenie zavedených systémov. V oblasti výskumu možno získať nové poznatky kombináciou veľkého množstva údajov a štatistických hodnotení, a to najmä v oblastiach, v ktorých do dnešného dňa bolo množstvo údajov vyhodnocovaných len manuálne. Môže dôjsť k vývoju nových liečebných postupov prispôbených jednotlivým pacientom na základe porovnania s množstvom dostupných informácií. Spoločnosti dúfajú, že analýza big data im umožní získať konkurenčnú výhodu, prinesie potenciálne úspory a vytvorí nové obchodné príležitosti poskytovania priamych, individualizovaných služieb zákazníkom. Vládne agentúry dúfajú, že dôjde k zlepšeniam v oblasti trestného súdnictva. V stratégii Komisie pre

986 Vývoj softvéru na spracúvanie big data je stále v počítačovej fáze. Napriek tomu postupne dochádza k vývoju analytických programov, najmä na analýzu hromadných údajov a informácií, ktoré sa týkajú činností jednotlivcov, v reálnom čase. Možnosť štruktúrovanej analýzy a spracúvania big data vytvorila nové prostriedky na profilovanie a cielenú reklamu. Európska komisia, oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Na ceste k prosperujúcemu hospodárstvu založenému na údajoch, COM (2014) 442 final, Brusel, 2. júla 2014; Informačný list Európskej komisie o reforme ochrany údajov v EÚ a veľkých dátach a Rada Európy, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 2.

987 Informačný list Európskej komisie o reforme ochrany údajov v EÚ a veľkých dátach.

988 Medzinárodná konferencia splnomocnencov pre ochranu údajov a súkromia (2014), Resolution on Big Data a Európska komisia, oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Na ceste k prosperujúcemu hospodárstvu založenému na údajoch, COM (2014) 442 final, Brusel, 2. júla 2014, s. 2; Informačný list Európskej komisie o reforme ochrany údajov v EÚ a veľkých dátach a Rada Európy, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 1.

digitálny jednotný trh v Európe sa uznáva potenciál dátových technológií, služieb a big data slúžiť ako katalyzátor hospodárskeho rastu, inovácie a digitalizácie v EÚ⁹⁸⁹.

Big data však so sebou prinášajú aj **riziká**, vo všeobecnosti súvisiace s tzv. atribútmi „3V“ (volume, velocity, variety): objem, rýchlosť a rozmanitosť spracúvaných údajov. Objem sa vzťahuje na množstvo spracúvaných údajov, rozmanitosť na počet a rôznorodosť druhov údajov, a rýchlosť sa týka rýchlosti spracúvania údajov. Osobitné dôvody na ochranu údajov vznikajú najmä vtedy, keď sa pri veľkých súboroch údajov používajú analýzy big data na získanie nových a prediktívnych znalostí na účely rozhodovania týkajúce sa jednotlivcov a/alebo skupín⁹⁹⁰. Riziká pre ochranu údajov a súkromia v súvislosti s big data boli zdôraznené v stanoviskách EDPS a pracovnej skupiny zriadenej podľa článku 29, uzneseniach Európskeho parlamentu a v dokumentoch Rady Európy⁹⁹¹.

Riziká môžu zahŕňať zneužívanie big data zo strany tých, ktorí manipuláciou, diskrimináciou alebo útlakom jednotlivcov alebo osobitných skupín v spoločnosti získajú prístup k veľkému objemu týchto informácií⁹⁹². Ak sa získavajú, spracúvajú a vyhodnocujú veľké objemy osobných údajov alebo informácií o individuálnom správaní, ich zneužívanie môže viesť k závažnému porušovaniu základných práv a slobôd, ktoré presahujú rámec práva na súkromie. Nie je možné presne zmerať rozsah, v akom môžu byť dotknuté súkromie a osobné údaje. Európsky parlament skonštatoval, že neexistuje metodika posudzovania celkových vplyvov big data na základe dôkazov, existujú však dôkazy o tom, že analýza big data môže mať významný horizontálny vplyv vo verejnom i súkromnom sektore⁹⁹³.

989 Uznesenie Európskeho parlamentu zo 14. marca 2017 o vplyve veľkých dát na základné práva: súkromie, ochrana údajov, nediskriminácia, bezpečnosť a presadzovanie práva (2016/2225 (INI)).

990 Rada Európy, Poradný výbor pre Dohovor č. 108, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 2.

991 Pozri napríklad, EPDS (2015), Čeliť výzvam tzv. *big data*, stanovisko 7/2015, Brusel, 19. novembra 2015; EDPS (2016), Účinné presadzovanie práv v digitálnej spoločnosti a ekonomike, stanovisko 8/2016, 23. septembra 2016; Európsky parlament (2016), Uznesenie o vplyve veľkých dát na základné práva: súkromie, ochrana údajov, nediskriminácia, bezpečnosť a presadzovanie práva, P8_TA(2017)0076, Štrasburg, 14. marca 2017; Rada Európy, Poradný výbor pre Dohovor č. 108, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, T-PD(2017)01, Štrasburg, 23. januára 2017.

992 Medzinárodná konferencia splnomocnencov pre ochranu údajov a súkromia (2014), Resolution on Big Data.

993 Uznesenie Európskeho parlamentu zo 14. marca 2017 o vplyve veľkých dát na základné práva: súkromie, ochrana údajov, nediskriminácia, bezpečnosť a presadzovanie práva (2016/2225 (INI)).

Všeobecné nariadenie o ochrane údajov obsahuje ustanovenia o práve osoby, aby sa na ňu nevzťahovalo automatizované rozhodovanie vrátane profilovania⁹⁹⁴. Ochrana súkromia sa stáva problematickou, keď si uplatňovanie práva namietat' vyžaduje ľudský zásah, ktorý by dotknutým osobám umožnil vyjadriť svoje stanovisko a napadnúť rozhodnutie⁹⁹⁵. Môžu tu vznikať problémy pri zabezpečovaní primeranej úrovne ochrany osobných údajov, napríklad, ak nie je možný ľudský zásah alebo ak sú algoritmy príliš zložité a množstvo príslušných údajov je príliš veľké na to, aby bolo jednotlivcom poskytnuté odôvodnenie určitých rozhodnutí a/alebo aby im boli poskytnuté informácie vopred s cieľom získať ich súhlas. Príkladom využitia umelej inteligencie a automatizovaného rozhodovania je najnovší vývoj v oblasti poskytovania hypoték alebo náborových procesov. Žiadosti sa zamietajú alebo im nie je vyhovie na základe skutočnosti, že žiadatelia nespĺňajú vopred určené parametre alebo faktory.

10.1.3. Otázky súvisiace s ochranou údajov

Pokiaľ ide o ochranu údajov, hlavné problémy sa týkajú na jednej strane objemu a rozmanitosti spracúvaných osobných údajov a na druhej strane spracúvania a jeho výsledkov. Využívaním komplexných algoritmov a softvéru sa z hromadných údajov stal zdroj na účely rozhodovania, a to má vplyv najmä na jednotlivcov a skupiny, predovšetkým v prípadoch profilovania alebo označovania, a v konečnom dôsledku to vyvoláva mnohé otázky týkajúce sa ochrany údajov⁹⁹⁶.

Identifikácia prevádzkovateľov a sprostredkovateľov a ich zodpovednosť

Big data a umelá inteligencia vyvolávajú niekoľko otázok vo vzťahu k identifikácii prevádzkovateľov a sprostredkovateľov a ich zodpovednosti: kto je vlastníkom údajov pri získavaní a spracúvaní tak veľkých množstiev údajov? Kto je prevádzkovateľom, keď údaje spracúvajú inteligentné stroje a softvér? Aké sú konkrétne oblasti zodpovednosti jednotlivých aktérov pri spracúvaní? A na aké účely sa môžu použiť big data?

994 Všeobecné nariadenie o ochrane údajov, článok 22.

995 Tamže, článok 22 ods. 3.

996 Rada Európy, Poradný výbor pre Dohovor č. 108, Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data, 23. januára 2017, s. 2.

Otázka zodpovednosti v súvislosti s umelou inteligenciou sa stane ešte problematickejšou, keď umelá inteligencia začne prijímať rozhodnutia na základe spracúvania údajov, ktoré vyvinula sama. Vo všeobecnom nariadení o ochrane údajov sa stanovuje právny rámec zodpovednosti prevádzkovateľa a sprostredkovateľa. Nezákonné spracúvanie osobných údajov vedie k vzniku zodpovednosti prevádzkovateľa a sprostredkovateľa⁹⁹⁷. Umelá inteligencia a automatizované rozhodovanie vyvolávajú otázky o tom, kto je zodpovedný za porušenia ovplyvňujúce súkromie dotknutých osôb v prípadoch, keď komplexnosť a množstvo spracúvaných údajov neumožňuje s istotou pripísať zodpovednosť. Ak sa umelá inteligencia a algoritmy považujú za produkty, vyvoláva to otázky týkajúce sa osobnej zodpovednosti, ktorá je upravená všeobecným nariadením o ochrane údajov, a zodpovednosti za výrobok, ktorá ním upravená nie je⁹⁹⁸. Chýbajú pravidlá v oblasti zodpovednosti, ktoré by napríklad vyplnili medzeru medzi osobnou zodpovednosťou a zodpovednosťou za výrobky v oblasti robotiky a umelej inteligencie vrátane automatizovaného rozhodovania⁹⁹⁹.

Vplyv na zásady ochrany údajov

Povaha, analýza a používanie vyššie opísaných big data nezodpovedajú uplatňovaniu niektorých tradičných základných zásad európskeho práva v oblasti ochrany údajov¹⁰⁰⁰. Problémy v tejto oblasti sa týkajú najmä zásady zákonnosti, minimalizácie údajov, obmedzenia účelu a transparentnosti.

Pri zásade minimalizácie údajov sa vyžaduje, aby osobné údaje boli primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Model zaobchádzania s big data však môže byť opakom minimalizácie údajov, pretože vyžaduje čoraz viac údajov, často na nešpecifikované účely.

To isté platí pri zásade obmedzenia účelu, pri ktorej sa vyžaduje, aby sa údaje spracúvali na konkrétne účely, a nemôžu sa použiť na účely, ktoré nie sú zlučiteľné s pôvodným účelom ich získania, pokiaľ takéto spracúvanie nie je založené na právnom základe – okrem iného na súhlase dotknutej osoby (pozri [oddiel 4.1.1](#)).

⁹⁹⁷ Všeobecné nariadenie o ochrane údajov, články 77 – 79 a článok 82.

⁹⁹⁸ Európsky parlament, Európske normy občianskeho práva v oblasti robotiky, generálne riaditeľstvo pre vnútornú politiku Únie, (október 2016), s. 14

⁹⁹⁹ Prejav Roberta Violu na mediálnom seminári o európskom zákone robotiky v Európskom parlamente. (PREJAV 16/02/2017); Oznámenie Európskeho parlamentu o žiadosti predloženej Komisii o návrh týkajúci sa noriem občianskoprávnej zodpovednosti v oblasti robotiky a UI.

¹⁰⁰⁰ Rada Európy, *Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo svete Big data*, T-PD (2017) 01, Štrasburg, 23. januára 2017.

Napokon, big data tiež nezodpovedajú zásade správnosti údajov, keďže aplikácie založené na big data získavajú údaje z rôznych zdrojov bez možnosti kontroly a/alebo zachovania správnosti získavaných údajov¹⁰⁰¹.

Osobitné pravidlá a práva

Nadálej platí všeobecné pravidlo, že osobné údaje spracúvané prostredníctvom analýzy big data patria do rozsahu pôsobnosti právnych predpisov o ochrane údajov. V právnych predpisoch EÚ a RE sa napriek tomu zaviedli osobitné pravidlá alebo výnimky týkajúce sa konkrétnych prípadov v súvislosti s algoritmickým komplexným spracúvaním údajov.

V rámci právnych predpisov RE sa modernizovaným Dohovorom č. 108 dotknutej osobe priznávajú nové práva s cieľom umožniť účinnejšiu kontrolu jej osobných údajov vo veku big data. Ide napríklad o článok 9 ods. 1 písm. a), c) a d) modernizovaného Dohovoru a konkrétne o právo ne byť predmetom rozhodnutia s významným vplyvom na dotknutú osobu výlučne na základe automatizovaného spracúvania údajov bez toho, aby sa zohľadnili názory dotknutej osoby; právo získať na požiadanie informácie o zdôvodnení spracúvania údajov, ak sa na dotknutú osobu vzťahujú výsledky takéhoto spracúvania, ako aj právo namietat'. Ďalšie ustanovenia modernizovaného Dohovoru č. 108, najmä pokiaľ ide o transparentnosť a dodatočné povinnosti, sú doplnkovými prvkami ochranného mechanizmu, ktorý sa v modernizovanom Dohovore č. 108 zavádza na riešenie digitálnych výziev.

V právnych predpisoch EÚ sa s výnimkou prípadov uvedených v článku 23 GDPR musí zabezpečiť **transparentnosť** pri každom spracúvaní osobných údajov. Je mimoriadne dôležitá, najmä pokiaľ ide o internetové služby a iné komplexné automatizované spracúvanie údajov, ako je používanie algoritmov pri rozhodovaní. Charakteristiky systémov spracúvania údajov musia dotknutým osobám umožňovať skutočne pochopiť, čo sa deje s ich údajmi. Vo všeobecnom nariadení o ochrane údajov na zabezpečenie spravodlivého a transparentného spracúvania sa vyžaduje, aby prevádzkovateľ poskytol dotknutej osobe zmysluplné informácie o logike automatizovaného rozhodovania vrátane profilovania¹⁰⁰². Výbor ministrov Rady Európy vo svojom odporúčaní o ochrane a podpore práva na slobodu prejavu a práva na súkromný život vo vzťahu k neutralite siete odporučil, aby poskytovatelia internetových služieb

¹⁰⁰¹ EDPS (2016), Účinné presadzovanie práv v digitálnej spoločnosti a ekonomike, stanovisko 8/2016, 23. septembra 2016, s. 8.

¹⁰⁰² Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. f).

„poskytovali používateľom jasné, úplné a verejne dostupné informácie o všetkých postupoch riadenia dátových tokov, ktoré môžu ovplyvniť prístup používateľov k obsahu, aplikáciám alebo službám a ich distribúciu“¹⁰⁰³. Správy o postupoch riadenia internetového dátového prenosu vypracované príslušnými orgánmi vo všetkých členských štátoch by mali byť vypracované otvorene a transparentne a verejnosti by sa mali sprístupniť bezplatne¹⁰⁰⁴.

Prevádzkovatelia musia **informovať** dotknuté osoby – keď údaje boli získané od nich alebo aj keď neboli – nielen o konkrétnych informáciách o získaných údajoch a plánovanom spracúvaní (pozri [oddiel 6.1.1](#)), ale v prípade potreby aj o existencii automatizovaných rozhodovacích procesov, a poskytnúť im „zmysluplné informácie o použitom postupe“¹⁰⁰⁵, cieľoch a potenciálnych dôsledkoch takýchto procesov. Vo všeobecnom nariadení o ochrane údajov sa takisto objasňuje (len v prípadoch, keď sa od dotknutej osoby nezískali osobné údaje), že prevádzkovateľ nie je povinný poskytnúť dotknutej osobe takéto informácie, ak „poskytnutie takýchto informácií by bolo nemožné alebo by si vyžadovalo neprimerané úsilie“¹⁰⁰⁶. Ako však zdôrazňuje pracovná skupina zriadená podľa článku 29 vo svojich *usmerneniach k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, zložitosť spracúvania by sama osebe nemala brániť tomu, aby prevádzkovateľ poskytoval dotknutej osobe jasné vysvetlenia o cieľoch a analýze použitej pri spracúvaní údajov¹⁰⁰⁷.

Práva dotknutých osôb na **prístup** k ich osobným údajom, ich **opravu** a **vymazanie**, ako aj ich právo na **obmedzenie** spracúvania, nezahŕňajú podobnú výnimku. Povinnosť prevádzkovateľa informovať dotknutú osobu o akejkoľvek oprave alebo vymazaní jej osobných údajov (pozri [oddiel 6.1.4](#)) sa však môže zrušiť aj vtedy, ak by sa takéto oznámenie „ukázalo ako nemožné možné alebo si vyžadovalo neprimerané úsilie“¹⁰⁰⁸.

1003 Rada Európy, Výbor ministrov (2016), Odporúčanie CM/Rec(2016)1 členským štátom o ochrane a podpore práva na slobodu prejavu a práva na súkromný život vo vzťahu k sieťovej neutralite, 13. januára 2016, bod 5.1.

1004 Tamže, bod 5.2.

1005 Všeobecné nariadenie o ochrane údajov, článok 13 ods. 2 písm. f) a článok 14 ods. 2 písm. g).

1006 Tamže, článok 14 ods. 5 písm. b).

1007 Pracovná skupina zriadená podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251, 3. októbra 2017, s. 14.

1008 Všeobecné nariadenie o ochrane údajov, článok 19.

Dotknuté osoby majú takisto právo **namietat** podľa článku 21 GDPR (pozri [oddiel 6.1.6](#)) pri akomkoľvek spracúvaní svojich osobných údajov vrátane prípadov analýzy big data. Hoci prevádzkovatelia môžu byť oslobodení od tejto povinnosti, ak preukážu nadradený oprávnený záujem, nemôžu využívať takéto oslobodenie pri spracúvaní na účely priameho marketingu.

V prípade spracúvania osobných údajov na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely môžu prevádzkovatelia takisto využiť osobitné výnimky z týchto práv¹⁰⁰⁹.

Pokiaľ ide o **profilovanie a automatizované rozhodovanie**, v GDPR sa zaviedli osobitné pravidlá: v článku 22 ods. 1 sa stanovuje, že dotknutá osoba „má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, [...] ktoré má právne účinky, ktoré sa jej týkajú“. Ako sa zdôrazňuje v usmerneniach pracovnej skupiny zriadenej podľa článku 29, v tomto článku sa uvádza všeobecný zákaz plne automatizovaného rozhodovania¹⁰¹⁰. Prevádzkovatelia môžu byť oslobodení od takéhoto zákazu len v troch špecifických prípadoch: ak je rozhodnutie: 1. nevyhnutné na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom; 2. povolené právom Únie alebo právom členského štátu alebo 3. založené na výslovnom súhlase¹⁰¹¹.

Individuálna kontrola

Zložitosť a nedostatočná transparentnosť v oblasti analýzy big data si môžu vyžadovať prehodnotenie myšlienok individuálnej kontroly osobných údajov. Túto kontrolu je potrebné prispôbiť danému sociálnemu a technologickému kontextu s prihliadnutím na nedostatok poznatkov zo strany jednotlivcov. Ochrana údajov v súvislosti s big data by preto mala zohľadniť širšiu myšlienku kontroly využívania údajov, na základe ktorej sa individuálna kontrola vyvinie do komplexnejšieho procesu viacnásobného posúdenia vplyvu rizík súvisiacich s používaním údajov¹⁰¹².

Kvalita aplikácie založenej na big data závisí od toho, do akej miery dokáže predpovedať želania alebo správanie testovaných jednotlivcov (alebo spotrebiteľov).

¹⁰⁰⁹ Tamže, článok 89 ods. 2 a 3.

¹⁰¹⁰ Pracovná skupina zriadená podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251, 3. októbra 2017, s. 9.

¹⁰¹¹ Všeobecné nariadenie o ochrane údajov, článok 22 ods. 2.

¹⁰¹² Rada Európy, Poradný výbor pre Dohovor č. 108, *Usmernenia o ochrane jednotlivcov so zreteľom na spracúvanie osobných údajov vo Big data*, T-PD(2017)01, Štrasburg, 23. januára 2017.

Súčasný prognostický model založený na analýze big data sa neustále zdokonaľujú. Najnovší vývoj zahŕňa nielen používanie údajov na kategorizáciu osobností (t. j. správania a postojov), ale aj analýzu správania na základe analýzy štruktúry hlasu a intenzity písania správ alebo telesnej teploty. Všetky tieto informácie možno využiť v reálnom čase na základe poznatkov získaných z vyhodnotenia big data, napríklad na posúdenie úverovej bonity počas stretnutia so zástupcom banky. Posúdenie sa nevykonáva na základe dojmu z jednotlivca podávajúceho žiadosť o úver, ale skôr na základe charakteristík správania vyplývajúcich z analýzy a vyhodnotenia informácií z big data, t. j. zvučný alebo lichotivý hlas žiadateľa, reč jeho tela alebo jeho telesná teplota.

Profilovanie a cieľná reklama nemusia byť nevyhnutne problematické, ak si jednotlivci **uvedomujú**, že sú vystavení reklame, ktorá im bola prispôbená na mieru. Profilovanie sa stáva problémom, keď sa používa na manipuláciu jednotlivcov, t. j. na vyhľadávanie určitých osobností alebo skupín ľudí na politickú kampaň. Napríklad skupiny nerozhodujúcich voličov možno osloviť politickým posolstvom, ktoré je prispôbené ich „osobnosti“ a postojom. Ďalším problémom by mohlo byť použitie takéhoto profilovania na odmietnutie prístupu určitých jednotlivcov k tovarom a službám. Jednou zo záruk, ktorá môže poskytnúť ochranu pred zneužitím big data a osobných informácií, je pseudonymizácia (pozri [oddiel 2.1.1](#))¹⁰¹³. Ak sú osobné údaje skutočne anonymizované, t. j. neexistujú žiadne stopy informácií, ktoré by boli prepojené s dotknutou osobou, tieto prípady nepatria do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov. Súhlas dotknutých osôb a jednotlivcov so spracúvaním big data je problematický aj z hľadiska právnych predpisov o ochrane údajov. Týka sa to súhlasu s tým, že sa na ne budú vzťahovať prispôbené reklamy a profilovanie, ktoré môže byť odôvodnené zlepšovaním „skúsenosti zákazníka“, a súhlasu s použitím veľkých objemov osobných údajov na zlepšenie a vývoj analytických nástrojov založených na informáciách. Informovanosť alebo nedostatočná informovanosť o spracúvaní big data vyvoláva niekoľko otázok v súvislosti s tým, ako môžu dotknuté osoby uplatniť svoje práva, keďže spracúvanie big data sa môže opierať o pseudonymizované. ako aj anonymizované informácie, ktoré sa využívajú v algoritmoch. Pseudonymizované údaje patria do všeobecného nariadenia o ochrane údajov, nariadenie sa však nevzťahuje na anonymizované údaje. Individuálna kontrola a informovanosť o spracúvaní osobných údajov sú pri analýze big data kľúčové: bez nich dotknuté osoby nebudú mať jasnú predstavu o tom, kto je prevádzkovateľ alebo sprostredkovateľ, čo im bude brániť v účinnom uplatňovaní ich práv.

1013 Tamže, s. 2.

10.2. Web 2.0 a web 3.0: sociálne siete a internet vecí

Hlavné body

- Služby sociálnych sietí sú online komunikačné platformy, ktoré umožňujú jednotlivcom pripojiť sa do sietí rovnako zmýšľajúcich používateľov alebo vytvoriť takéto siete.
- Internet vecí znamená pripojenie predmetov na internet a vzájomné prepojenie predmetov.
- Súhlas dotknutých osôb je najbežnejším právnym základom na zákonné spracúvanie údajov prevádzkovateľmi na sociálnych sieťach.
- Používatelia sociálnych sietí sú vo všeobecnosti chránení výnimkou pre domáce činnosti; táto výnimka však za určitých okolností nemusí platiť.
- Poskytovatelia sociálnych sietí nie sú chránení výnimkou domácej činnosti.
- Špecificky navrhnutá a štandardná ochrana údajov je nevyhnutná na zaistenie bezpečnosti údajov v tejto oblasti.

10.2.1. Vymedzenie pojmu web 2.0 a web 3.0

Služby sociálnych sietí

Internet bol pôvodne vytvorený ako sieť na vzájomné prepojenie počítačov a na prenos správ s obmedzenými kapacitami na výmenu údajov, pričom webové sídla len ponúkali jednotlivcom pasívne prezeranie ich obsahu¹⁰¹⁴. S nástupom veku Web 2.0 sa internet transformoval na fórum, na ktorom sú používatelia vo vzájomnom kontakte, spolupracujú a prispievajú vstupmi. Tento vek sa vyznačuje pozoruhodným úspechom a rozsiahlym využívaním služieb sociálnych sietí, ktoré sú v súčasnosti nevyhnutnou súčasťou každodenného života miliónov ľudí.

Služby sociálnych sietí (SSS) alebo sociálne médiá je možné vo všeobecnosti vymedziť ako „online komunikačné platformy, ktoré umožňujú jednotlivcom pripojiť sa do sietí rovnako zmýšľajúcich používateľov alebo vytvoriť takéto siete“¹⁰¹⁵. Pri pripojení

¹⁰¹⁴ Európska komisia (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

¹⁰¹⁵ Pracovná skupina zriadená podľa článku 29 (2009), *Stanovisko 5/2009 k sociálnym sieťam on-line*, WP 163, 12. júna 2009, s. 4.

sa k sieti alebo vytváraní siete sa od jednotlivcov vyžaduje, aby poskytli osobné údaje a vytvorili si svoj profil. SSS umožňujú užívateľom vytvárať digitálny „obsah“, od fotografií a videa až po odkazy na novinové články a osobné príspevky, v ktorých vyjadrujú svoje názory. Prostredníctvom týchto online komunikačných platforiem môžu používatelia nadväzovať kontakt a komunikovať s viacerými ďalšími používateľmi. Čo je dôležité, pri väčšine obľúbených SSS sa neplatia žiadne registračné poplatky. Poskytovatelia SSS namiesto toho, aby vyžadovali úhradu za pripojenie sa do siete, dosahujú väčšinu svojich príjmov z cieľenej reklamy. Zadávatelia reklamy značne profitujú z osobných informácií, ktoré sa na týchto stránkach denne objavujú. Informácie o veku, pohlaví, polohe a záujmoch používateľa im umožňujú, aby svojou reklamou oslovili tých „správnych“ ľudí.

Výbor ministrov Rady Európy prijal [odporúčanie o ochrane ľudských práv vo vzťahu k službám sociálnych sietí](#)¹⁰¹⁶, ktoré sa v osobitnej časti zaoberá ochranou údajov a v roku 2018 bolo doplnené ďalším odporúčaním o úlohách a povinnostiach sprostredkovateľov (intermediaries) prístupu na internet¹⁰¹⁷.

Príklad: Nora je veľmi šťastná, pretože ju jej partner požiadal o ruku. Chce sa podeliť o dobrú správu so svojimi priateľmi a rodinou a rozhodne sa napísať emocionálny príspevok na sociálnej sieti, v ktorom vyjadrí svoju radosť, a zmeniť svoj status na „zasnúbená“. V nasledujúcich dňoch Nora po prihlásení do svojho účtu vidí reklamy na svadobné šaty a kvetinárstva. Ako je to možné?

Pri vytváraní reklamy na sieti Facebook si spoločnosti predávajúce svadobné šaty a kvetinárstva vybrali určité parametre, aby mohli osloviť ľudí ako Nora. Ak z Norinho profilu vyplýva, že je žena, ktorá je zasnúbená, žije v Paríži, v blízkosti oblasti, kde sa nachádzajú tieto obchody so šatami a kvetinárstva, reklama sa jej okamžite bude zobrazovať.

Internet vecí

Internet vecí predstavuje ďalší krok vo vývoji internetu: vek Web 3.0. Internet vecí umožňuje pripojenie zariadení a vzájomnú interakciu s inými zariadeniami

¹⁰¹⁶ Rada Európy, Výbor ministrov, Odporúčanie CM/Rec(2012)4 Výboru ministrov členským štátom o ochrane ľudských práv v súvislosti so službami sociálnych sietí, 4. apríla 2012.

¹⁰¹⁷ Rada Európy, Výbor ministrov (2001), Odporúčanie CM/Rec(2018)2 členským štátom o úlohách a povinnostiach sprostredkovateľov prístupu na internet, 7. marca 2018.

prostredníctvom internetu. Umožňuje sa tým vzájomné prepojenie predmetov a ľudí prostredníctvom komunikačných sietí, aby mohli informovať o svojom stave a/alebo stave okolitého prostredia¹⁰¹⁸. Internet vecí a pripojené zariadenia sú už realitou a očakáva sa, že v najbližších rokoch sa budú ďalej rozvíjať, a to vytvorením a ďalším rozvojom inteligentných zariadení, ktoré povedú k vytvoreniu inteligentných miest, inteligentných domácností a inteligentných podnikov.

Príklad: Internet vecí môže byť obzvlášť prínosný v oblasti zdravotnej starostlivosti. Spoločnosti už vytvorili zariadenia, senzory a aplikácie, ktoré umožňujú monitorovanie zdravia pacienta. Nositeľné poplachové tlačidlá a iné bezdrôtové senzory umiestnené v domácnosti umožňujú sledovanie každodenného života starších ľudí, ktorí žijú sami, a vyslať varovania, ak sa zistí závažné narušenie ich dennej rutiny. Starší ľudia napríklad vo veľkej miere využívajú senzory, ktoré upozornia, ak dôjde k pádu. Tieto senzory dokážu presne identifikovať, že došlo k pádu, a upozorniť lekára a/alebo rodinného príslušníka.

Príklad: Jedným z najznámejších príkladov inteligentného mesta je Barcelona. Od roku 2012 zaviedlo mesto využívanie inováčných technológií s cieľom vytvoriť inteligentný systém verejnej dopravy, nakladania s odpadom, parkovania a pouličného osvetlenia. Napríklad na zlepšenie nakladania s odpadom mesto využíva inteligentné odpadové nádoby. Umožňujú monitorovanie úrovni odpadu s cieľom optimalizovať trasy zberu. Ak sú nádoby takmer plné, vysielajú prostredníctvom mobilnej komunikačnej siete signály, ktoré prijíma softvérová aplikácia, ktorú používa podnik zodpovedný za nakladanie s odpadom. Podnik tak môže naplánovať tú najlepšiu cestu na zber odpadu, pričom uprednostňuje a/alebo organizuje zber odpadu len pre tie nádoby, ktoré je skutočne potrebné vyprázdniť.

10.2.2. Vyvažovanie výhod a rizík

Obrovské rozšírenie a úspech služieb sociálnych sietí v poslednom desaťročí naznačuje, že poskytujú **významné výhody**. Napríklad cielená reklama (ako je opísaná vo vyznačenom príklade) je obzvlášť inovatívnym spôsobom oslovovania publika, ktorý spoločnostiam ponúka konkrétnejšie vymedzený trh. Aj spotrebiteľ by mohli

¹⁰¹⁸ Európska komisia, pracovný dokument útvarov Komisie, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19. apríla 2016.

oceniť, že sa im budú zobrazovať reklamy, ktoré sú relevantnejšie a zaujímavejšie. Čo je však dôležitejšie, služby sociálnych sietí a sociálne médiá môžu mať pozitívny vplyv na spoločnosť a pri zavádzaní zmien. Umožňujú používateľom komunikáciu, interakciu, organizovanie skupín a podujatí týkajúcich sa záležitostí, ktoré sú pre nich dôležité.

Podobne sa očakáva, že internet vecí bude predstavovať významný prínos pre hospodárstvo, pričom je súčasťou stratégie EÚ zameranej na rozvoj digitálneho jednotného trhu. Odhaduje sa, že v roku 2020 sa počet pripojení k internetu vecí zvýši na šesť miliárd. Očakáva sa, že toto rozšírenie pripojiteľnosti prinesie významné hospodárske výhody vo forme rozvoja inovačných služieb a aplikácií, lepšej zdravotnej starostlivosti, lepšieho pochopenia potrieb spotrebiteľov a zvýšenej efektívnosti.

Vzhľadom na obrovské množstvo osobných informácií, ktoré vytvárajú používatelia sociálnych médií a následne ich spracúvajú prevádzkovatelia služieb, rozširovanie SSS vyvoláva čoraz väčšie obavy v súvislosti so spôsobmi ochrany súkromia a osobných údajov. Služby sociálnych sietí môžu ohroziť právo na súkromný život a právo na slobodu prejavu. Takéto hrozby môžu zahŕňať: „nedostatok právnych a procesných záruk súvisiacich s procesmi, ktoré môžu viesť k vylúčeniu používateľov; nedostatočná ochrana detí a mladých ľudí pred škodlivým obsahom alebo správaním; nedostatočné rešpektovanie práv iných; chýbajúce štandardné nastavenia ochrany súkromia; nedostatočná transparentnosť, pokiaľ ide o účely, na ktoré sa osobné údaje získavajú a spracúvajú“¹⁰¹⁹. Európske právne predpisy o ochrane údajov sa snažili reagovať na výzvy v oblasti ochrany súkromia a ochrany údajov, ktoré so sebou prinášajú sociálne médiá. Zásady ako súhlas, špecificky navrhnutá a štandardná ochrana súkromia/údajov a práva jednotlivcov sú mimoriadne dôležité v kontexte sociálnych médií a sieťových služieb.

V kontexte internetu vecí veľký objem osobných údajov pochádzajúcich z rôznych vzájomne prepojených zariadení so sebou prináša aj riziká pre súkromie a ochranu údajov. Hoci transparentnosť je dôležitou zásadou európskych právnych predpisov v oblasti ochrany údajov, pri takom veľkom počte pripojených zariadení nie je vždy jasné, kto je schopný získavať údaje zozbierané zo zariadení internetu vecí, získať prístup k nim a využívať ich¹⁰²⁰. V právnych predpisoch EÚ a Rady Európy sa však zásadou transparentnosti stanovuje prevádzkovateľom povinnosť jasne

1019 Rada Európy, Odporúčanie Rec(2012)4 členským štátom o ochrane ľudských práv v súvislosti so službami sociálnych sietí, 4. apríla 2012.

1020 Európsky dozorný úradník pre ochranu údajov (2017), *Understanding the Internet of Things*.

a jednoducho informovať dotknuté osoby o tom, ako sa ich údaje používajú. Musia dotknutým osobám objasniť riziká, pravidlá, záruky a práva týkajúce sa spracúvania ich osobných údajov. Zariadenia pripojené na internet vecí a mnohé spracovateľské operácie a dotknuté údaje môžu byť tiež problematické z hľadiska požiadavky jasného a informovaného súhlasu so spracúvaním údajov – ak je takéto spracúvanie založené na súhlase. Jednotlivci často nechápu technické fungovanie takeéhoto spracúvania, a teda nechápu ani dôsledky svojho súhlasu.

Ďalšou veľkou obavou je bezpečnosť vzhľadom na to, že pripojené zariadenia sú osobitne ohrozené bezpečnostnými rizikami. Pripojené zariadenia majú rôzne úrovne bezpečnosti. Keďže fungujú mimo rámca štandardnej IT infraštruktúry, nemusia mať dostatočný výkon na spracúvanie ani pamäťovú kapacitu na umiestnenie bezpečnostného softvéru alebo využívanie techník, ako je šifrovanie, pseudonymizácia alebo anonymizácia na ochranu osobných informácií používateľov.

Príklad: V Nemecku regulačné orgány rozhodli o zákaze hračky pripojenej na internet po tom, ako sa objavili vážne obavy týkajúce sa vplyvu hračky na rešpektovanie súkromného života detí. Regulačné orgány usúdili, že bábika s pripojením na internet pomenovaná Cayla v podstate funguje ako skryté sledovacie zariadenie. Bábika zasielala zvukové nahrávky otázok dieťaťa, ktoré sa s ňou hralo, aplikácii na digitálnom zariadení, ktorá ich preložila do textovej formy a našla odpoveď na internete. Aplikácia následne zaslala odpoveď bábike, ktorá dieťaťu povedala odpoveď. Prostredníctvom tejto bábiky by sa komunikácia dieťaťa, ako aj komunikácia dospelých osôb v blízkosti mohla zaznamenať a prenášať do aplikácie. Ak by výrobcovia bábiky neprijali primerané bezpečnostné opatrenia, bábiku mohol ktokoľvek použiť na odpočúvanie rozhovorov.

10.2.3. Otázky súvisiace s ochranou údajov

Súhlas

V Európe je spracúvanie osobných údajov zákonné len vtedy, ak je povolené podľa európskych právnych predpisov o ochrane údajov. Pokiaľ ide o poskytovateľov služieb sociálnych sietí, súhlas dotknutých osôb vo všeobecnosti predstavuje zákonný základ na spracúvanie údajov. Súhlas sa musí poskytnúť slobodne a musí byť

konkrétny, informovaný a jednoznačný (pozri [oddiel 4.1.1](#))¹⁰²¹. „Slobodne poskytnutý“ v podstate znamená, že dotknuté osoby musia byť schopné skutočne a naozaj si vybrať. Súhlas je „konkrétny“ a „informovaný“, ak je zrozumiteľný, pričom jasne a presne odkazuje na úplný rozsah, účely a dôsledky spracúvania údajov. V súvislosti so sociálnymi médiami je možné spochybniť, či je súhlas slobodný, konkrétny a informovaný pre všetky typy spracúvania, ktoré vykonáva prevádzkovateľ SSS a tretie strany.

Príklad: Ak sa chcú jednotlivci pripojiť do SSS a mať k nim prístup, často musia súhlasiť s rôznymi druhmi spracúvania svojich osobných údajov, často bez toho, aby im boli poskytnuté potrebné podrobnosti alebo alternatívne možnosti. Príkladom je potreba poskytnúť súhlas s prijímaním behaviorálnej reklamy, aby sa bolo možné zaregistrovať do SSS. Ako uvádza pracovná skupina zriadená podľa článku 29 vo svojom stanovisku k definícii súhlasu, „vzhľadom na význam, aký získali niektoré sociálne siete, niektoré kategórie používateľov (ako tínedžeri) prejavia súhlas s prijímaním behaviorálnej reklamy, aby sa vyhli riziku, že budú čiastočne vylúčení zo sociálnych interakcií. Používatelovi by sa mala ponúknuť pozícia, v ktorej môže poskytnúť slobodný a konkrétny súhlas s prijímaním behaviorálnej reklamy, nezávisle od jeho prístupu k službe sociálnej siete“¹⁰²².

Podľa všeobecného nariadenia o ochrane údajov sa osobné údaje detí do 16 rokov v zásade nemôžu spracúvať na základe ich súhlasu¹⁰²³. Ak je súhlas na spracúvanie potrebný, musí ho poskytnúť rodič dieťaťa alebo opatrovník dieťaťa. Deti si zasluhujú osobitnú ochranu, keďže si môžu byť v menšej miere vedomé rizík a dôsledkov spojených so spracúvaním údajov. Je to veľmi dôležité v kontexte sociálnych médií, pretože deti sú zraniteľnejšie, pokiaľ ide o niektoré negatívne účinky používania takýchto médií, ako je kybernetické šikanovanie, online prenasledovanie alebo krádež totožnosti.

¹⁰²¹ Všeobecné nariadenie o ochrane údajov, články 4 a 7; modernizovaný Dohovor č. 108, článok 5.

¹⁰²² Pracovná skupina zriadená podľa článku 29 (2011), *Stanovisko 15/2011 k definícii súhlasu*, WP 187, 13. júla 2011, s. 18.

¹⁰²³ Pozri všeobecné nariadenie o ochrane údajov, článok 8. Členské štáty EÚ môžu právnymi predpismi stanoviť nižší vek za predpokladu, že nie je nižší ako 13 rokov.

Bezpečnosť a špecificky navrhnutá a štandardná ochrana súkromia/údajov

Spracúvanie osobných údajov samo o sebe zahŕňa bezpečnostné riziká vzhľadom na neustálu možnosť narušenia bezpečnosti, ktorá by mohlo viesť k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo sprístupneniu spracúvaných osobných údajov, alebo neoprávnenému prístupu k nim. Podľa európskych právnych predpisov o ochrane údajov sú prevádzkovatelia a sprostredkovatelia povinní prijať primerané technické a organizačné opatrenia, aby zabránili akémukoľvek neoprávnenému zasahovaniu do operácií spracúvania údajov. Túto povinnosť musia spĺňať aj poskytovatelia služieb sociálnych sietí, ktorí patria do rozsahu pôsobnosti európskych pravidiel ochrany údajov.

V zásadách špecificky navrhnutej a štandardnej ochrany súkromia/údajov sa od prevádzkovateľov vyžaduje, aby zachovávali bezpečnosť pri navrhovaní svojich produktov a aby automaticky uplatňovali vhodné nastavenia ochrany súkromia a údajov. Znamená to, že ak sa osoba rozhodne pripojiť do sociálnej siete, poskytovateľ služieb nemusí automaticky sprístupniť všetky informácie o novom používateľovi služieb všetkým svojim používateľom. Pri pripojení sa k službe by štandardné nastavenia ochrany súkromia a údajov mali byť také, aby informácie boli dostupné len pre kontakty, ktoré si jednotlivец vybral. Rozšírenie prístupu na osoby mimo tohto zoznamu by malo byť možné, len ak používateľ manuálne zmení štandardné nastavenia ochrany súkromia a údajov. Môže to ovplyvniť aj prípady, keď dôjde k porušeniu ochrany údajov napriek zavedeniu bezpečnostných opatrení. V takýchto prípadoch musia poskytovatelia služieb upovedomiť príslušných používateľov, ak je pravdepodobné, že porušenie povedie k vysokému riziku pre práva a slobody dotknutej osoby¹⁰²⁴.

Špecificky navrhnutá a štandardná ochrana súkromia/údajov je osobitne dôležitá v kontexte SSS, keďže okrem rizík neoprávneného prístupu, ktoré sa týkajú väčšiny druhov spracúvania, výmena osobných informácií na sociálnych médiách predstavuje dodatočné bezpečnostné riziká. Často je to v dôsledku toho, že jednotlivci nemajú predstavu o tom, kto má prístup k ich informáciám a ako by ich mohol využiť. S rozšíreným využívaním sociálnych médií narastá počet prípadov krádeže totožnosti a obetí týchto krádeží.

1024 Tamže, článok 34.

Príklad: O krádeži totožnosti hovoríme, keď osoba získa informácie, údaje alebo dokumenty patriace inej osobe (obeti) a následne použije tieto informácie na to, aby obeť napodobnila a získala tak v jej mene tovary alebo služby. Uvedme príklad Pavla, ktorý má konto na stránke sociálnych médií. Pavol je učiteľ a aktívny člen komunity, je veľmi spoločenský a jeho nastavenia ochrany súkromia a osobných údajov na jeho konte na sociálnych médiách ho veľmi netrápia. Jeho zoznam kontaktov je rozsiahly, niekedy vrátane ľudí, ktorých ani nemusí osobne poznať. Vzhľadom na to, že pracuje vo veľkej škole a je pomerne populárny, keďže je trénerom školského futbalového družstva, predpokladá, že ide o ľudí, ktorí sú s najväčšou pravdepodobnosťou rodičmi alebo priateľmi školy. Pavol má na svojom konte na sociálnych médiách zobrazenú svoju e-mailovú adresu a dátum narodenia. Okrem toho Pavol pravidelne zverejňuje fotografie svojho psa Tobyho, ku ktorým pridáva poznámku ako „Môj ranný beh s Tobym“. Paul si neuvedomil, že jednou z najpopulárnejších bezpečnostných otázok na ochranu e-mailového konta alebo mobilného telefónu je otázka „ako sa volá vaše domáce zvieratko“. Na základe informácií, ktoré sú dostupné na Pavlovom profile na sociálnych médiách, Dominik jednoducho dokáže získať neoprávnený prístup k Pavlovým kontám.

Práva jednotlivcov

Poskytovatelia služieb sociálnych sietí musia rešpektovať práva jednotlivcov (pozri [oddiel 6.1](#)) vrátane práva byť informovaný o účele spracúvania a o tom, ako sa môžu osobné údaje použiť na účely priameho marketingu. Jednotlivci musia mať tiež právo na prístup k osobným údajom, ktoré vytvorili na platforme sociálnych sietí, a právo požadovať ich vymazanie. Aj v prípade, že osoby súhlasili so spracúvaním osobných údajov a poskytli informácie online, mali by mať možnosť požiadať o „zabudnutie“, ak už nechcú využívať služby sociálnej siete. Právo na prenosnosť údajov ďalej umožňuje používateľom získať kópiu osobných údajov, ktoré poskytli poskytovateľovi sociálnych sietí, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a preniesť svoje údaje inému poskytovateľovi služieb sociálnych sietí¹⁰²⁵.

¹⁰²⁵ Všeobecné nariadenie o ochrane údajov, článok 21.

Prevádzkovatelia

V súvislosti so sociálnymi médiami sa často objavuje zložitá otázka, kto je prevádzkovateľom, a teda: kto má povinnosť a zodpovednosť dodržiavať pravidlá ochrany údajov. Poskytovatelia služieb sociálnych sietí sa považujú za prevádzkovateľov v zmysle európskych právnych predpisov o ochrane údajov. Je to zrejme vzhľadom na široké vymedzenie pojmu „prevádzkovateľ“ a skutočnosť, že títo poskytovatelia služieb určujú účel a prostriedky spracúvania osobných údajov, ktoré uvádzajú jednotlivci. Podľa právnych predpisov EÚ platí, že ak prevádzkovatelia poskytujú služby dotknutým osobám v EÚ, musia dodržiavať ustanovenia všeobecného nariadenia o ochrane údajov, aj keď nie sú usadené v EÚ.

Môžu sa však za prevádzkovateľov považovať aj používatelia služieb sociálnych sietí? Ak jednotlivci spracúvajú osobné údaje „v priebehu výlučne osobnej alebo domácej činnosti“, pravidlá ochrany údajov sa neuplatňujú. V európskych právnych predpisoch o ochrane údajov sa hovorí o „výnimke pre domáce činnosti“. V niektorých prípadoch sa však táto výnimka pre domáce činnosti nemusí vzťahovať na používateľa služby sociálnej siete.

Používatelia dobrovoľne zverejňujú svoje osobné informácie na internete. Informácie zverejňované na internete však často zahŕňajú aj osobné informácie iných jednotlivcov.

Príklad: Pavol má účet na veľmi populárnej platforme sociálnej siete. Pavol sa chce stať hercom a využíva svoj účet na zverejňovanie fotografií, videí a príspevkov, v ktorých vysvetľuje svoje zanievanie pre umenie. Pre jeho budúcnosť je dôležité, aby bol populárny, a preto sa rozhodol, že jeho profil by mal byť viditeľný nielen pre jeho úzky okruh kontaktov, ale pre všetkých používateľov internetu bez ohľadu na to, či sú členmi tejto siete alebo nie. Môže Pavol zverejňovať fotografie a videá, na ktorých je so svojou priateľkou Sárrou, bez jej súhlasu? Sára je učiteľka na základnej škole a snaží sa neposkytovať informácie o svojom súkromnom živote svojmu zamestnávateľovi, študentom a ich rodičom. Predstavte si prípad, že Sára, ktorá nepoužíva sociálne siete, zistí od spoločného priateľa Dominika, že Pavol na internete zverejnil fotografiu, na ktorej sú s Pavlom na večierku. V takom prípade sa na Pavlovo spracúvanie údajov nevzťahujú právne predpisy EÚ, pretože sa uplatňuje „výnimka pre domáce činnosti“.

Pre používateľov je však naďalej rozhodujúce, aby si uvedomovali, že zverejňovanie informácií o iných osobách bez ich súhlasu môže predstavovať porušovanie práv týchto jednotlivcov na ochranu súkromia a údajov. Aj v prípade, keď sa uplatňuje výnimka pre domáce činnosti, napríklad, ak má používateľ profil, ktorý sa zverejňuje len skupine kontaktov, ktoré si vybral, zverejnenie osobných informácií o iných osobách by aj tak mohlo viesť k zodpovednosti používateľa. Hoci pravidlá ochrany údajov by sa neuplatňovali, ak by platila výnimka pre domáce činnosti, zodpovednosť by mohla vyplývať z uplatňovania iných vnútroštátnych pravidiel, ako je ohovárание alebo porušenie práv na ochranu osobnosti. Výnimka pre domáce činnosti sa vzťahuje len na používateľov služieb sociálnych sietí: prevádzkovatelia a sprostredkovatelia, ktorí poskytujú prostriedky na takéto súkromné spracúvanie, podliehajú právnym predpisom EÚ o ochrane údajov¹⁰²⁶.

S reformou smernice o súkromí a elektronických komunikáciách by sa pravidlá ochrany údajov, súkromia a bezpečnosti, ktoré sa uplatňujú na poskytovateľov telekomunikačných služieb na základe súčasného právneho rámca, uplatňovali aj na komunikáciu stroj-stroj a elektronické komunikačné služby vrátane napríklad over-the-top služieb.

¹⁰²⁶ Tamže, odôvodnenie 18.

Odporúčaná literatúra

Kapitola 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*, Viedeň, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance“, *International Data Privacy Law*, zv. 6, č. 3, s. 195 – 209.

EDRi, *An introduction to data protection*, Brusel.

Frowein, J. a Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

González Fuster, G. a 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*, zv. 26 (1), s. 73 – 82.

Grabenwarter, C. a Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Mníchov, C. H. Beck.

Gutwirth, S., Poulet, Y., de Hert, P., de Terwange, C. a Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. a 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*, Mnichov, C. H. Beck.

Kokott, J. a Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ESJP“, *International Data Privacy Law*, zv. 3, č. 4, s. 222 – 228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten“, *European Data Protection Law Review*, zv. 1, č. 1, s. 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*, zv. 63, č. 3, s. 569 – 597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, 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. a Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antverpy, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. a Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brusel, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?“, *Neue Juristische Wochenschrift*, č. 5, s. 281 – 288.

Warren, S. a Brandeis, L. (1890), „[The right to privacy](#)“, *Harvard Law Review*, zv. 4, č. 5, s. 193 – 220.

White, R. a Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Kapitola 2

Acquisty, A., a Gross R. (2009), „[Predicting Social Security numbers from public data](#)“, *Proceedings of the National Academy of Science*, 7. júla 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., a Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility“, *Nature Scientific Reports*, zv. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paríž, 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. a Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londýn, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“, *UCLA Law Review*, zv. 57, č. 6, s. 1701 – 1777.

Samarati, P. a Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“, Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy“ *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, zv. 10, č. 5, s. 557 – 570.

Tinnefeld, M., Buchner, B. a Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Mnichov, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Kapitoly 3 až 6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ in: Grabitz, E., Hilf, M. a Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Mnichov, 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. a Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?“, *Computer Law & Security Review*, zv. 26, č. 3 s. 273 – 283.

Dammann, U. a Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. a Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“, *Computers & Law Magazine of SCL*, zv. 22, č. 6, s. 1 – 5.

De Hert, P. a 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*, zv. 28, č. 2, s. 130 – 142.

Feretti, Federico (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*, zv. 20, č. 2, s. 473 – 506.

FRA (Agentúra Európskej únie pre základné práva) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburg, Úrad pre vydávanie publikácií Európskej únie (Úrad pre publikácie).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Viedeň, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburg, Úrad pre publikácie.

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. a Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108“, *Computer Law & Security Review*, zv. 27, č. 3, s. 223 – 231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner’s Office, [Privacy Impact Assessment](#).

Kapitola 7

Európsky dozorný úradník pre ochranu údajov (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. a Nouwt, S. (2009), *Reinventing data protection?*, Berlín, 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.

Pracovná skupina zriadená podľa článku 29 (2005), [Pracovný dokument o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995](#).

Kapitola 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londýn, 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*, Berlín, Springer.

De Hert, P. a Papakonstantinou, V. (2012), „[The Police and Criminal Justice Data Protection Directive: Comment and Analysis](#)“, *Computers & Law Magazine of SCL*, zv. 22, č. 6, s. 1 – 5.

Drewer, D. a Ellermann, J. (2012), „Europol’s data protection framework as an asset in the fight against cybercrime“, *ERA Forum*, zv. 13, č. 3, s. 381 – 395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxemburg, Úrad pre publikácie.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlín, Springer.

Gutwirth, S., Pouillet, Y. a De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Pouillet, Y., De Hert, P. a 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*, zv. 36, č. 5, s. 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 Working Papers 2013/2.

Kapitola 9

Büllesbach, A., Gijrath, S., Poulet, Y. a Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. a Poulet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y. a De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poulet, Y., De Hert, P. a 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*, zv. 36, č. 5, s. 722 – 776.

Rosemary, J. a Hamilton, A. (2012), *Data protection law and practice*, Londýn, Sweet & Maxwell.

Kapitola 10

El Emam, K. a Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques“, *International Data Privacy Law*, zv. 5, č. 1, s. 73 – 87.

Mayer-Schönberger, V. a Cate, F. (2013), „Notice and consent in a world of Big Data“, *International Data Privacy Law*, zv. 3, č. 2, s. 67 – 73.

Rubinstein, I. (2013), „Big Data: The End of Privacy or a New Beginning?“, *International Data Privacy Law*, zv. 3, č. 2, s. 74 – 87.

Judikatúra

Vybraná judikatúra Európskeho súdu pre ľudské práva

Prístup k osobným údajom

Gaskin/Spojené kráľovstvo, č. 10454/83, 7. júla 1989

Godelli/Taliansko, č. 33783/09, 25. septembra 2012

K.H. a i./Slovensko, č. 32881/04, 28. apríla 2009

Leander/Švédsko, č. 9248/81, 26. marca 1987

M.K./Francúzsko, č. 19522/09, 18. apríla 2013

Odièvre/Francúzsko [VK], č. 42326/98, 13. februára 2003

Vyvažovanie ochrany údajov so slobodou prejavu a právom na informácie

Axel Springer AG/Nemecko [VK], č. 39954/08, 7. februára 2012

Bohlen/Nemecko, č. 53495/09, 19. februára 2015

Couderc a Hachette Filipacchi Associés/Francúzsko [VK], č. 40454/07, 10. novembra 2015

Magyar Helsinki Bizottság/Maďarsko [VK], č. 18030/11, 8. novembra 2016

Müller a i./Švajčiarsko, č. 10737/84, 24. mája 1988

Satakunnan Markkinapörssi Oy a Satamedia Oy/Fínsko, č. 931/13, 27. júna 2017

Vereinigung bildender Künstler/Rakúsko, č. 68354/01, 25. januára 2007

Von Hannover/Nemecko (č. 2), [VK], č. 40660/08 a 60641/08, 7. februára 2012

Vyvažovanie ochrany údajov so slobodou náboženstva

Sinan Işık/Turecko, č. 21924/05, 2. februára 2010

Výzvy v oblasti ochrany údajov online

K.U./Fínsko, č. 2872/02, 2. decembra 2008

Súhlas dotknutej osoby

Elberte/Lotyšsko, č. 61243/08, 13. januára 2015

Sinan Isık/Turecko, č. 21924/05, 2. februára 2010

Y/Turecko, č. 648/10, 17. februára 2015

Korešpondencia

Amann/Švajčiarsko [VK], č. 27798/95, 16. februára 2000

Association for European Integration and Human Rights a Ekimdziev/Bulharsko, č. 62540/00, 28. júna 2007

Bernh Larsen Holding AS a i./Nórsko, č. 24117/08, 14. marca 2013

Cemalettin Canli/Turecko, č. 22427/04, 18. novembra 2008

D.L./Bulharsko, č. 7472/14, 19. mája 2016

Dalea/Francúzsko, č. 964/07, 2. februára 2010

Gaskin/Spojené kráľovstvo, č. 10454/83, 7. júla 1989

Haralambie/Rumunsko, č. 21737/03, 27. októbra 2009

Khelili/Švajčiarsko, č. 16188/07, 18. októbra 2011

Leander/Švédsko, č. 9248/81, 26. marca 1987

Malone/Spojené kráľovstvo, č. 8691/79, 2. augusta 1984

Rotaru/Rumunsko [VK], č. 28341/95, 4. mája 2000

S. a Marper/Spojené kráľovstvo [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008

Silver a i./Spojené kráľovstvo, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marca 1983

Šimovolos/Rusko, č. 30194/09, 21. júna 2011

The Sunday Times/Spojené kráľovstvo, č. 6538/74, 26. apríla 1979

Databázy registra trestov

Aycaguer/Francúzsko, č. 8806/12, 22. júna 2017

B.B./Francúzsko, č. 5335/06, 17. decembra 2009

Brunet/Francúzsko, č. 21010/10, 18. septembra 2014

M.K./Francúzsko, č. 19522/09, 18. apríla 2013

M.M./Spojené kráľovstvo, č. 24029/07, 13. novembra 2012

Bezpečnosť osobných údajov

Haralambie/Rumunsko, č. 21737/03, 27. októbra 2009

K.H. a i./Slovensko, č. 32881/04, 28. apríla 2009

Databázy DNA

S. a Marper/Spojené kráľovstvo [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008

Údaje GPS

Uzun/Nemecko, č. 35623/05, 2. septembra 2010

Údaje týkajúce sa zdravia

Avilkina a i./Rusko, č. 1585/09, 6. júna 2013

Biriuk/Litva, č. 23373/03, 25. novembra 2008

I/Fínsko, č. 20511/03, 17. júla 2008

L.H./Lotyšsko, č. 52019/07, 29. apríla 2014

L.L./Francúzsko, č. 7508/02, 10. októbra 2006

M.S./Švédsko, č. 20837/92, 27. augusta 1997

Szuluk/Spojené kráľovstvo, č. 36936/05, 2. júna 2009

Y/Turecko, č. 648/10, 17. februára 2015

Z/Fínsko, č. 22009/93, 25. februára 1997

Totožnosť

Ciubotaru/Moldavsko, č. 27138/04, 27. apríla 2010

Godelli/Taliansko, č. 33783/09, 25. septembra 2012

Odièvre/Francúzsko [VK], č. 42326/98, 13. februára 2003

Informácie týkajúce sa profesijnej činnosti

G.S.B./Švajčiarsko, č. 28601/11, 22. decembra 2015

M.N. a i./San Maríno, č. 28005/12, 7. júla 2015

Michaud/Francúzsko, č. 12323/11, 6. decembra 2012

Niemietz/Nemecko, č. 13710/88, 16. decembra 1992

Odpočúvanie komunikácie

Amann/Švajčiarsko [VK], č. 27798/95, 16. februára 2000

Brito Ferrinho Bexiga Villa-Nova/Portugalsko, č. 69436/10, 1. decembra 2015

Copland/Spojené kráľovstvo, č. 62617/00, 3. apríla 2007

Halford/Spojené kráľovstvo, č. 20605/92, 25. júna 1997

Iordachi a i./Moldavsko, č. 25198/02, 10. februára 2009

Kopp/Švajčiarsko, č. 23224/94, 25. marca 1998

Liberty a i./Spojené kráľovstvo, č. 58243/00, 1. júla 2008

Malone/Spojené kráľovstvo, č. 8691/79, 2. augusta 1984

Mustafa Sezgin Tanrikulu/Turecko, č. 27473/06, 18. júla 2017

Pruteanu/Rumunsko, č. 30181/05, 3. februára 2015

Szuluk/Spojené kráľovstvo, č. 36936/05, 2. júna 2009

Povinnosti zodpovedných subjektov

B.B./Francúzsko, č. 5335/06, 17. decembra 2009

I/Fínsko, č. 20511/03, 17. júla 2008

Mosley/Spojené kráľovstvo, č. 48009/08, 10. mája 2011

Osobné údaje

Amann/Švajčiarsko [VK], č. 27798/95, 16. februára 2000

Bernh Larsen Holding AS a i./Nórsko, č. 24117/08, 14. marca 2013

Uzun/Nemecko, č. 35623/05, 2010

Fotografie

Sciacca/Taliansko, č. 50774/99, 11. januára 2005

Von Hannover/Nemecko, č. 59320/00, 24. júna 2004

Právo na zabudnutie

Satakunnan Markkinapörssi Oy a Satamedia Oy/Fínsko, č. 931/13, 27. júna 2017

Segerstedt-Wiberg a i./Švédsko, č. 62332/00, 6. júna 2006

Právo namietať

Leander/Švédsko, č. 9248/81, 26. marca 1987

M.S./Švédsko, č. 20837/92, 27. augusta 1997

Mosley/Spojené kráľovstvo, č. 48009/08, 10. mája 2011

Rotaru/Rumunsko [VK], č. 28341/95, 4. mája 2000

Sinan Işık/Turecko, č. 21924/05, 2. februára 2010

Citlivé kategórie údajov

Brunet/Francúzsko, č. 21010/10, 18. septembra 2014

I/Fínsko, č. 20511/03, 17. júla 2008

Michaud/Francúzsko, č. 12323/11, 6. decembra 2012

S. a Marper/Spojené kráľovstvo [VK], č. 30562/04 a č. 30566/04, 4. decembra 2008

Dohľad a presadzovanie (úloha rôznych subjektov vrátane dozorných orgánov)

I/Fínsko, č. 20511/03, 17. júla 2008

K.U./Fínsko, č. 2872/02, 2. decembra 2008

Von Hannover/Nemecko, č. 59320/00, 24. júna 2004

Von Hannover/Nemecko (č. 2), [VK], č. 40660/08 a 60641/08, 7. februára 2012

Metódy sledovania

Allan/Spojené kráľovstvo, č. 48539/99, 5. novembra 2002
Association for European Integration and Human Rights a Ekimdžiev/Bulharsko,
 č. 62540/00, 28. júna 2007
Bărbulescu/Rumunsko [VK], č. 61496/08, 5. septembra 2017
D.L./Bulharsko, č. 7472/14, 19. mája 2016
Dragojević/Chorvátsko, č. 68955/11, 15. januára 2015
Karabeyoğlu/Turecko, č. 30083/10, 7. júna 2016
Klass a i./Nemecko, č. 5029/71, 6. septembra 1978
Roman Zakharov/Rusko [VK], č. 47143/06, 4. decembra 2015
Rotaru/Rumunsko [VK], č. 28341/95, 4. mája 2000
Szabó a Vissy/Maďarsko, č. 37138/14, 12. januára 2016
Taylor-Sabori/Spojené kráľovstvo, č. 47114/99, 22. októbra 2002
Uzun/Nemecko, č. 35623/05, 2. septembra 2010
Versini-Campinchi a Crasnianski/Francúzsko, č. 49176/11, 16. júna 2016
Vetter/Francúzsko, č. 59842/00, 31. mája 2005
Vukota-Bojić/Švajčiarsko, č. 61838/10, 18. októbra 2016

Monitorovanie kamerou

Köpke/Nemecko, č. 420/07, 5. októbra 2010
Peck/Spojené kráľovstvo, č. 44647/98, 28. januára 2003

Vzorky hlasu

P.G. a J.H./Spojené kráľovstvo, č. 44787/98, 25. septembra 2001
Wisse/Francúzsko, č. 71611/01, 20. decembra 2005

Vybraná judikatúra Súdneho dvora Európskej únie

Judikatúra súvisiaca so smernicou o ochrane údajov

Spojené veci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, 24. novembra 2011

[Správne vykonávanie článku 7 písm. f) smernice o ochrane údajov – „oprávnené záujmy iných“ – vo vnútroštátnych právnych predpisoch]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/Netlog NV*, 16. februára 2012

[Povinnosť poskytovateľov sociálnych sietí zabrániť užívateľom siete, aby nezákonne používali hudobné a audiovizuálne diela]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/ Salvatore Manni*, 9. marca 2017

[Právo na vymazanie osobných údajov; právo namietat' proti spracúvaniu]

C-553/07, *College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer*, 7. mája 2009

[Právo dotknutej osoby na prístup k údajom]

C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5. mája 2011

[Nevyhnutnosť nového súhlasu]

Spojené veci C-293/12 a C-594/12, *Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources a i. a Kärntner Landesregierung a i. [VK]*, 8. apríla 2014

[Porušenie primárneho práva EÚ smernicou o uchovávaní údajov; zákonné spracúvanie; obmedzenie účelu a minimalizácia uchovávanía]

C-288/12, *Európska komisia/Maďarsko [VK]*, 8. apríla 2014

[Legitímnosť zrušenia funkcie vnútroštátneho dozorného úradníka pre ochranu údajov]

C-614/10, *Európska komisia/Rakúska republika [VK]*, 16. októbra 2012

[Nezávislosť vnútroštátneho dozorného orgánu]

- C-518/07, *Európska komisia/Spolková republika Nemecko* [VK], 9. marca 2010
[Nezávislosť vnútroštátneho dozorného orgánu]
- C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11. decembra 2014
[Pojem „spracúvanie údajov“ a „prevádzkovateľ“]
- C-131/12, *Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* [VK], 13. mája 2014
[Povinnosti poskytovateľov vyhľadávačov na žiadosť dotknutej osoby nezobrazovať osobné údaje vo výsledkoch vyhľadávania; uplatniteľnosť smernice o ochrane údajov; pojem „spracúvania údajov“; význam pojmu „prevádzkovateľa“; vyvažovanie ochrany údajov so slobodou prejavu; právo na zabudnutie]
- C-524/06, *Heinz Huber/Bundesrepublik Deutschland* [VK], 16. decembra 2008
[Legitímnosť uchovávanía údajov o cudzincoch v štatistickom registri]
- C-473/12, *Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert a i.*, 7. novembra 2013
[Právo na informovanie o spracúvaní osobných údajov]
- C-362/14, *Maximilian Schrems/Data Protection Commissioner* [VK], 6. októbra 2015
[Zásada zákonného spracúvania; základné práva; neplatnosť rozhodnutia o Safe Harbour; právomoci nezávislých dozorných orgánov]
- C-291/12, *Michael Schwarz/Stadt Bochum*, 17. októbra 2013
[Návrh na začatie prejudiciálneho konania; priestor slobody, bezpečnosti a spravodlivosti; biometrický cestovný pas; odtlačky prstov; právny základ; primeranosť]
- C-582/14, *Patrick Breyer/Bundesrepublik Deutschland*, 19. októbra 2016
[Pojem „osobné údaje“; adresy internetového protokolu; uchovávanie údajov poskytovateľom online mediálnych služieb; vnútroštátna právna úprava, ktorá neumožňuje zohľadnenie oprávneného záujmu sledovaného prevádzkovateľom]
- C-434/16, *Peter Nowak/Data Protection Commissioner*, návrhy, ktoré predniesla generálna advokátka Kokott, 20. júla 2017
[Pojem osobné údaje; prístup k vlastným odpovediam na otázky na skúške; opravy skúšajúceho]

T-462/12 R, *Pilkington Group Ltd/Európska komisia*, uznesenie predsedu Všeobecného súdu, 11. marca 2013

C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU* [VK], 29. januára 2008

[Povinnosť poskytovateľov internetového pripojenia zverejniť totožnosť používateľov programov na výmenu súborov KaZaA združeniu na ochranu práv duševného vlastníctva]

Spojené veci C-465/00, C-138/01 a C-139/01, *Rechnungshof/Österreichischer Rundfunk a i. a Christa Neukomm a Joseph Lauer mann/Österreichischer Rundfunk*, 20. mája 2003

[Primeranosť právnej povinnosti uverejňovať osobné údaje o platoch zamestnancov určitých kategórií inštitúcií súvisiacich s verejným sektorom]

C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011

[Informačná spoločnosť; autorské právo; internet; programy „peer-to-peer“; poskytovatelia internetového pripojenia; zavedenie systému filtrovania elektronickej komunikácie s cieľom zabrániť výmene súborov porušujúcich autorské práva; neexistencia všeobecnej povinnosti monitorovať prenášané informácie]

C-201/14, *Smaranda Bara a i./Casa Națională de Asigurări de Sănătate a i.*, 1. októbra 2015

[Právo na informovanie o spracúvaní osobných údajov]

Spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.* [VK], 21. decembra 2016.

[Dôvernosť elektronickej komunikácie; poskytovatelia elektronických komunikačných služieb; povinnosť všeobecného a nediferencovaného uchovávanía prevádzkových a lokalizačných údajov; neexistencia predbežného preskúmania zo strany súdu alebo nezávislého správneho orgánu; Charta základných práv Európskej únie; zlučiteľnosť s právom Únie]

C-73/07, *Tietosuoja-valtuutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy* [VK], 16. decembra 2008

[Pojem „žurnalistické činnosti“ v zmysle článku 9 smernice o ochrane údajov]

SDEÚ, C-101/01, *Trestné konanie proti Bodil Lindqvist*, 6. novembra 2003.

[Osobitné kategórie osobných údajov]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde/Rīgas pašvaldības SIA „Rīgas satiksme”*, 4. mája 2017

[Zásada zákonného spracúvania: oprávnený záujem sledovaný treťou stranou]

Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen* [VK], 9. novembra 2010

[Pojem „osobné údaje“; primeranosť právnej povinnosti zverejňovať osobné údaje prijímateľov prostriedkov z určitých poľnohospodárskych fondov EÚ]

C-230/14, *Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. októbra 2015

[Právomoci vnútroštátnych dozorných orgánov]

C-342/12, *Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT)*, 30. mája 2013

[Pojem „osobné údaje“; záznamy o pracovnom čase; zásady týkajúce sa kvality údajov a zákonnosti spracúvania údajov; prístup vnútroštátneho orgánu príslušného v oblasti dohľadu nad pracovnými podmienkami; povinnosť zamestnávateľa sprístupniť záznamy o pracovnom čase spôsobom umožňujúcim do nich bezprostredne nahliadnuť]

Spojené veci C-141/12 a C-372/12, *YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S*, 17. júla 2014

[Rozsah práva dotknutej osoby na prístup; ochrana fyzických osôb pri spracúvaní osobných údajov; pojem „osobné údaje“; údaje týkajúce sa žiadateľa o povolenie na pobyt a právne analýzy obsiahnuté v správnom dokumente na účely prípravy rozhodnutia; Charta základných práv Európskej únie]

Judikatúra súvisiaca so smernicou 2016/681

Stanovisko 1/15 Súdneho dvora (veľká komora), 26. júla 2017

[Právny základ; návrh dohody medzi Kanadou a Európskou úniou o prenose a spracúvaní údajov z osobného záznamu o cestujúcom; zlučiteľnosť návrhu dohody s článkom 16 ZFEÚ a článkami 7 a 8 a článkom 52 ods. 1 Charty základných práv Európskej únie]

Judikatúra súvisiaca s nariadením o ochrane údajov inštitúciami EÚ

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe)/Európsky úrad pre bezpečnosť potravín (EFSA), Európska komisia*, 16. júla 2015

[Prístup k dokumentom]

C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd.* [VK], 29. júna 2010
[Prístup k dokumentom]

Judikatúra súvisiaca so smernicou 2002/58/ES

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

[Autorské právo a s ním súvisiace práva; spracúvanie údajov cez internet; porušenie výlučného práva; audioknihy, ktoré boli cez internet sprístupnené prostredníctvom servera FTP, na ktorý boli zaslané z adresy IP pridelennej poskytovateľom internetu; súdny príkaz adresovaný poskytovateľovi internetu oznámiť meno a adresu používateľa s určitou adresou IP]

C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. novembra 2011

[Informačná spoločnosť; autorské právo; internet; programy „peer-to-peer“; poskytovatelia internetového pripojenia; zavedenie systému filtrovania elektronickej komunikácie s cieľom zabrániť výmene súborov porušujúcich autorské práva; neexistencia všeobecnej povinnosti monitorovať prenášané informácie]

C-536/15, *Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)*, 15. marca 2017.

[Zásada nediskriminácie; sprístupnenie osobných údajov účastníkov na účely poskytovania verejne dostupných telefónnych informačných služieb a služieb telefónnych zoznamov; súhlas účastníka; rozlišovanie podľa členského štátu, v ktorom sa verejne dostupná telefónna informačná služba a služba telefónnych zoznamov poskytujú]

Spojené veci C-203/15 a C-698/15, *Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.* [VK], 21. decembra 2016.

[Dôvernoscť elektronickej komunikácie; poskytovatelia elektronických komunikačných služieb; povinnosť všeobecného a nediferencovaného uchovávanía prevádzkových a lokalizačných údajov; neexistencia predbežného preskúmania zo strany súdu alebo nezávislého správneho orgánu; Charta základných práv Európskej únie; zlučiteľnosť s právom Únie]

Index

Judikátúra Súdneho dvora Európskej únie

- Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)*
a Federación de Comercio Electrónico y Marketing Directo (FECEDM)/
Administración del Estado, spojené veci C-468/10 a C-469/10,
24. november 2011 32, 56, 146, 148, 163, 164
- Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)/*
Netlog NV, C-360/10, 16. februára 2012 79
- Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB,*
Storyside AB/Perfect Communication Sweden AB, C-461/10, 19. apríla 2012 79
- Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce/Salvatore*
Manni, C-398/15, 9. marca 2017 19, 81, 86, 103, 212, 213, 234, 239
- ClientEarth, Pesticide Action Network Europe (PAN Europe)/Európsky úrad pre*
bezpečnosť potravín (EFSA), Európska komisia, C-615/13 P,
16. júla 2015 18, 69, 225
- College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer,*
C-553/07, 7. mája 2009 121, 134, 212, 227
- Deutsche Telekom AG/Bundesrepublik Deutschland*, C-543/09,
5. mája 2011 87, 145, 154
- Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural*
Resources a i. a Kärntner Landesregierung a i. [VK],
spojené veci C-293/12 a C-594/12,
8. apríla 2014... 23, 48, 50, 64, 121, 122, 132, 137, 250, 251, 252, 282, 306, 307, 362

<i>Európska komisia/Maďarsko</i> [VK], C-288/12, 8. apríla 2014	195, 201
<i>Európska komisia/Rakúska republika</i> [VK], C-614/10, 16. október 2012.....	195, 201
<i>Európska komisia/Spolková republika Nemecko</i> [GC], C-518/07, 9. marca 2010...	195, 200
<i>Európska komisia/The Bavarian Lager Co. Ltd.</i> [VK], C-28/08 P, 29. júna 2010.....	18, 67, 213, 250
<i>František Ryneš/Úřad pro ochranu osobních údajů</i> , C-212/13, 11. december 2014.....	86, 97, 103, 109
<i>Google Spain SL a Google Inc./Agencia Española de Protección de Datos (AEPD) a Mario Costeja González</i> [VK], C-131/12, 13. Mája 2014	18, 19, 59, 60, 80, 86, 104, 110, 111, 212, 232, 233, 234, 238
<i>Heinz Huber/Bundesrepublik Deutschland</i> [VK], C-524/06, 16. decembra 2008	145, 148, 159, 160, 337, 354
<i>Institut professionnel des agents immobiliers (IPI)/Geoffrey Englebert a i.</i> , C-473/12, 7. novembra 2013.....	211, 216
<i>International Transport Workers' Federation a Finnish Seamen's Union/Viking Line ABP a OÜ Viking Line Eesti</i> [VK], C-438/05, 11. decembra 2007	252
<i>Maximilian Schrems/Data Protection Commissioner</i> [VK], C-362/14, 6. októbra 2015....	47, 195, 197, 198, 203, 213, 248, 250, 259, 264, 265, 266, 270, 271
<i>Michael Schwarz/Stadt Bochum</i> , C-291/12, 17. októbra 2013.....	52, 54
<i>Pasquale Foglia/Mariella Novello</i> (č. 2), C-244/80, 16. decembra 1981	252
<i>Patrick Breyer/Bundesrepublik Deutschland</i> , C-582/14, 19. októbra 2016	85, 96
<i>Peter Nowak/Data Protection Commissioner</i> , C-434/16, návrhy, ktoré predniesla generálna advokátka Kokott, 20. júla 2017	86, 212
<i>Pilkington Group Ltd/Európska komisia</i> , T-462/12 R, uznesenie predsedu Všeobecného súdu, 11. marca 2013.....	72
<i>Productores de Música de España (Promusicae)/Telefónica de España SAU</i> [VK], C-275/06, 29. januára 2008	19, 56, 77, 80, 85, 94
<i>Rechnungshof/Österreichischer Rundfunk a i. a Christa Neukomm a Joseph Lauerermann/Österreichischer Rundfunk</i> , spojené veci C-465/00, C-138/01 a C-139/01, 20. mája 2003.....	66, 148

<i>Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)</i> , C-70/10, 24. novembra 2011	46, 85, 94, 96
<i>Smaranda Bara a i./Președintele Casei Naționale de Asigurări de Sănătate a i.</i> , C-201/14, 1. októbra 2015	95, 121, 128, 211, 217, 358
<i>Stanovisko 1/15 Súdneho dvora (velká komora)</i> , 26. júla 2017	46, 277
<i>Tele2 (Netherlands) BV a i./Autoriteit Consument en Markt (ACM)</i> , C-536/15, 15. marca 2017	87, 145, 154, 155
<i>Tele2 Sverige AB/Post- och telestyrelsen a Secretary of State for the Home Department/Tom Watson a i.</i> [VK], spojené veci C-203/15 a C-698/15, 21. decembra 2016	46, 50, 64, 282, 308
<i>Tietosuoja-valtuutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy</i> [VK], C-73/07, 16. decembra 2008	18, 57
<i>Trestné konanie proti Bodil Lindqvist</i> , C-101/01, 6. novembra 2003	85, 86, 101, 104, 109, 177
<i>Trestné konanie proti Giuseppe Francesco Gasparini a iní.</i> , C-467/04, 28. septembra 2006	252
<i>Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen</i> [VK], spojené veci C-92/09 a C-93/09, 9. novembra 2010	18, 21, 39, 49, 65, 85, 90, 91
<i>Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság</i> , C-230/14, 1. októbra 2015	204
<i>Worten – Equipamentos para o Lar, SA/Autoridade para as Condições de Trabalho (ACT)</i> , C-342/12, 30. mája 2013	343
<i>YS/Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel/M a S</i> , spojené veci C-141/12 a C-372/12, 17. júla 2014	85, 91, 95, 212, 225
Judikatura Európskeho súdu pre ľudské práva	
<i>Allan/Spojené kráľovstvo</i> , č. 48539/99, 5. novembra 2002	281, 286
<i>Amann/Švajčiarsko</i> [VK], č. 27798/95, 16. februára 2000	40, 85, 91, 93
<i>Association for European Integration and Human Rights a Ekimdziev/Bulharsko</i> , č. 62540/00, 28. júna 2007	41
<i>Avilkina a i./Rusko</i> , č. 1585/09, 6. júna 2013	349
<i>Axel Springer AG/Nemecko</i> [VK], č. 39954/08, 7. februára 2012	18, 60
<i>Aycaguer/Francúzsko</i> , č. 8806/12, 22. júna 2017	285

<i>B.B./Francúzsko</i> , č. 5335/06, 17. decembra 2009.....	281, 282, 285
<i>Bărbulescu/Rumunsko</i> [VK], č. 61496/08, 5. septembra 2017.....	92, 345
<i>Bernh Larsen Holding AS a i./Nórsko</i> , č. 24117/08, 14. marca 2013.....	85, 89
<i>Biriuk/Litva</i> , č. 23373/03, 25. novembra 2008.....	63, 213, 349
<i>Bohlen/Nemecko</i> , č. 53495/09, 19. februára 2015.....	18, 62
<i>Brito Ferrinho Bexiga Villa-Nova/Portugalsko</i> , č. 69436/10, 1. decembra 2015.....	72
<i>Brunet/Francúzsko</i> , č. 21010/10, 18. septembra 2014.....	230
<i>Cemalettin Canli/Turecko</i> , č. 22427/04, 18. novembra 2008.....	212, 229
<i>Ciubotaru/Moldavsko</i> , č. 27138/04, 27. apríla 2010.....	212, 228
<i>Copland/Spojené kráľovstvo</i> , č. 62617/00, 3. apríla 2007.....	26, 337, 344
<i>Couderc a Hachette Filipacchi Associés/Francúzsko</i> [VK], č. 40454/07, 10. novembra 2015.....	61
<i>D.L./Bulharsko</i> , č. 7472/14, 19. mája 2016.....	284
<i>Dalea/Francúzsko</i> , č. 964/07, 2. februára 2010.....	229, 282, 322
<i>Dragojević/Chorvátsko</i> , č. 68955/11, 15. januára 2015.....	284
<i>Elberte/Lotyšsko</i> , č. 61243/08, 2015.....	87
<i>G.S.B./Švajčiarsko</i> , č. 28601/11, 22. decembra 2015.....	357
<i>Gaskin/Spojené kráľovstvo</i> , č. 10454/83, 7. júla 1989.....	225
<i>Godelli/Taliansko</i> , č. 33783/09, 25. septembra 2012.....	225
<i>Halford/Spojené kráľovstvo</i> , č. 20605/92, 25. júna 1997.....	356
<i>Haralambie/Rumunsko</i> , č. 21737/03, 27. októbra 2009.....	121, 126
<i>I./Fínsko</i> , č. 20511/03, 17. júla 2008.....	26, 146, 174, 348
<i>Iordachi a i./Moldavsko</i> , č. 25198/02, 10. februára 2009.....	40
<i>K.H. a i./Slovensko</i> , č. 32881/04, 28. apríla 2009.....	121, 124, 225, 348
<i>K.U./Fínsko</i> , č. 2872/02, 2. decembra 2008.....	26, 213, 253, 262
<i>Karabeyoğlu/Turecko</i> , č. 30083/10, 7. júna 2016.....	247, 289
<i>Khelili/Švajčiarsko</i> , č. 16188/07, 18. októbra 2011.....	43
<i>Klass a i./Nemecko</i> , č. 5029/71, 6. septembra 1978.....	25, 26, 281, 283
<i>Köpke/Nemecko</i> , č. 420/07, 5. októbra 2010.....	97, 253
<i>Kopp/Švajčiarsko</i> , č. 23224/94, 25. marca 1998.....	40

<i>L.H./Lotyšsko</i> , č. 52019/07, 29. apríla 2014.....	349
<i>L.L./Francúzsko</i> , č. 7508/02, 10. októbra 2006	348
<i>Leander/Švédsko</i> , č. 9248/81, 26. marca 1987	42, 45, 212, 225, 238, 285
<i>Liberty a i./Spojené kráľovstvo</i> , č. 58243/00, 1. júla 2008	89
<i>M.K./Francúzsko</i> , č. 19522/09, 18. apríla 2013	230, 285
<i>M.M./Spojené kráľovstvo</i> , č. 24029/07, 13. novembra 2012.....	136, 285
<i>M.N. a i./San Maríno</i> , č. 28005/12, 7. júla 2015.....	95, 356
<i>M.S./Švédsko</i> , č. 20837/92, 27. augusta 1997	238, 348
<i>Magyar Helsinki Bizottság/Maďarsko [VK]</i> , č. 18030/11, 8. novembra 2016	18, 70
<i>Malone/Spojené kráľovstvo</i> , č. 8691/79, 2. augusta 1984.....	26, 40, 281
<i>Michaud/Francúzsko</i> , č. 12323/11, 6. decembra 2012.....	338, 356
<i>Mosley/Spojené kráľovstvo</i> , č. 48009/08, 10. mája 2011	18, 62, 238
<i>Müller a i./Švajčiarsko</i> , č. 10737/84, 24. mája 1988.....	76
<i>Mustafa Sezgin Tanriku/Turecko</i> , č. 27473/06, 18. júla 2017.....	26, 247
<i>Niemietz/Nemecko</i> , č. 13710/88, 16. decembra 1992.....	92, 356
<i>Odièvre/Francúzsko [VK]</i> , č. 42326/98, 13. februára 2003.....	225
<i>P.G. a J.H./Spojené kráľovstvo</i> , č. 44787/98, 25. septembra 2001	97
<i>Peck/Spojené kráľovstvo</i> , č. 44647/98, 28. januára 2003	42, 97
<i>Pruteanu/Rumunsko</i> , č. 30181/05, 3. februára 2015.....	19, 72
<i>Roman Zakharov/Rusko [VK]</i> , č. 47143/06, 4. decembra 2015.....	26, 287
<i>Rotaru/Rumunsko [VK]</i> , č. 28341/95, 4. mája 2000	25, 41, 92, 229, 283
<i>S. a Marper/Spojené kráľovstvo [VK]</i> , č. 30562/04 a č. 30566/04, 4. decembra 2008.....	18, 39, 44, 122, 136, 281, 282, 285
<i>Satakunnan Markkinapörssi Oy a Satamedia Oy/Fínsko [VK]</i> , č. 931/13, 27. júna 2017	20, 58
<i>Sciacca/Taliansko</i> , č. 50774/99, 11. januára 2005	97
<i>Segerstedt-Wiberg a i./Švédsko</i> , č. 62332/00, 6. júna 2006	212, 230
<i>Silver a i./Spojené kráľovstvo</i> , č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. marca 1983.....	40
<i>Šimovolos/Rusko</i> , č. 30194/09, 21. júna 2011	41
<i>Sinan Işık/Turecko</i> , č. 21924/05, 2. februára 2010.....	74

<i>Szabó a Vissy/Maďarsko</i> , č. 37138/14, 12. januára 2016	25, 26, 281, 283, 287
<i>Szuluk/Spojené kráľovstvo</i> , č. 36936/05, 2. júna 2009	348
<i>Taylor-Sabori/Spojené kráľovstvo</i> , č. 47114/99, 22. októbra 2002	41
<i>The Sunday Times/Spojené kráľovstvo</i> , č. 6538/74, 26. apríla 1979	40
<i>Uzun/Nemecko</i> , č. 35623/05, 2. septembra 2010	26, 85
<i>Vereinigung bildender Künstler/Rakúsko</i> , č. 68345/01, 25. januára 2007	19, 76
<i>Versini-Campinchi a Crasnianski/Francúzsko</i> , č. 49176/11, 16. júna 2016	288
<i>Vetter/Francúzsko</i> , č. 59842/00, 31. mája 2005	41, 281
<i>Von Hannover/Nemecko (č. 2)</i> , [VK], č. 40660/08 a 60641/08, 7. februára 2012	56
<i>Von Hannover/Nemecko</i> , č. 59320/00, 24. júna 2004	97
<i>Vukota-Bojić/Svajčiarsko</i> , č. 61838/10, 18. októbra 2016	41
<i>Wisse/Francúzsko</i> , č. 71611/01, 20. decembra 2005	97
<i>Y/Turecko</i> , č. 648/10, 17. februára 2015	146, 165
<i>Z/Fínsko</i> , č. 22009/93, 25. februára 1997	28, 337, 348

Judikatúra vnútroštátnych súdov

Česká republika, Ústavný súd (<i>Ústavní soud České republiky</i>), 94/2011 Zb., 22. marca 2011	306
Nemecko, Spolkový ústavný súd (<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. decembra 1983	20
Nemecko, Spolkový ústavný súd (<i>Bundesverfassungsgericht</i>), 1 BvR 256/08, 2. marca 2010	306
Rumunsko, Federálny ústavný súd (<i>Curtea Constituțională a României</i>), č. 1258, 8. októbra 2009	306

Veľké množstvo informácií o Agentúre Európskej únie pre základné práva je k dispozícii na internete. Sú dostupné na webovej stránke FRA: fra.europa.eu

Ďalšie informácie o judikatúre Európskeho súdu pre ľudské práva sú k dispozícii na jeho webovej stránke: echr.coe.int. Vyhľadávací portál HUDOC umožňuje prístup k rozsudkom a rozhodnutiam v angličtine a/alebo vo francúzštine, prekladom do vybraných jazykov, stručným informáciám o prejednávanych prípadoch, tlačovým správam a ďalším informáciám o práci súdu.

Ako získať publikácie Rady Európy

Nakladateľstvo Rady Európy vydáva texty vo všetkých oblastiach pôsobnosti tejto organizácie vrátane ľudských práv, právnej vedy, zdravia, etiky, sociálnych vecí, životného prostredia, vzdelávania, kultúry, športu, mládeže a architektonického dedičstva. Knihy a elektronické publikácie z rozsiahleho katalógu si môžete objednať online (<http://book.coe.int/>).

Virtuálna čítareň umožňuje používateľom bezplatne nahliadnuť do výťahov z nedávno publikovaných hlavných diel alebo úplných textov určitých oficiálnych dokumentov.

Informácie o dohovoroch Rady Európy, ako aj ich úplné texty sú k dispozícii na webovej stránke Oddelenia pre dohovory: <http://conventions.coe.int/>

Obráťte sa na EÚ

Osobne

V rámci celej EÚ existujú stovky informačných centier Europe Direct. Adresu centra najbližšieho k vám nájdete na tejto webovej stránke: https://europa.eu/european-union/contact_sk

Telefónicky alebo e-mailom

Europe Direct je služba, ktorá odpovedá na vaše otázky o Európskej únii. Túto službu môžete kontaktovať:

- prostredníctvom bezplatného telefónneho čísla: 00 800 6 7 8 9 10 11 (niektorí operátori môžu tieto hovory spoplatňovať),
- prostredníctvom štandardného telefónneho čísla: +32 22999696, alebo
- e-mailom na tejto webovej stránke: https://europa.eu/european-union/contact_sk

Vyhľadávanie informácií o EÚ

Online

Informácie o Európskej únii sú dostupné vo všetkých úradných jazykoch Európskej únie na webovej stránke Europa: https://europa.eu/european-union/index_sk

Publikácie EÚ

Publikácie EÚ, bezplatné alebo platené, si môžete stiahnuť alebo objednať z kníhkupectva na webovej stránke <https://op.europa.eu/sk/publications>. Ak chcete získať viac než jeden výtlačok bezplatných publikácií, obráťte sa na službu Europe Direct alebo vaše miestne informačné centrum (pozri https://europa.eu/european-union/contact_sk).

Právo EÚ a súvisiace dokumenty

Prístup k právnym informáciám EÚ vrátane všetkých právnych predpisov EÚ od roku 1952 vo všetkých úradných jazykoch nájdete na webovej stránke EUR-Lex: <http://eur-lex.europa.eu>

Otvorený prístup k údajom z EÚ

Portál otvorených dát EÚ (<http://data.europa.eu/euodp/sk>) poskytuje prístup k súborom dát z EÚ. Dáta možno stiahnuť a opätovne použiť bezplatne na komerčné aj nekomerčné účely.

Rýchly rozvoj informačných technológií ešte viac zvýšil potrebu prísnej ochrany osobných údajov, pričom toto právo zaručujú ako nástroje Európskej únie (EÚ), tak aj Rady Európy. Zabezpečenie tohto dôležitého práva so sebou prináša nové a významné výzvy, keďže technologickým pokrokom sa rozširujú hranice možností v oblastiach, ako je sledovanie, odpočúvanie komunikácie a uchovávanie údajov. Cieľom tejto príručky je oboznámiť príslušníkov právnického povolania, ktorí sa nešpecializujú na ochranu údajov, s touto vznikajúcou oblasťou práva. Príručka obsahuje prehľad platných právnych rámcov EÚ a Rady Európy. Vysvetľuje sa v nej aj kľúčová judikatúra so zhrnutím dôležitých rozhodnutí Súdneho dvora Európskej únie (SDEÚ), ako aj Európskeho súdu pre ľudské práva (ESLP). Okrem toho obsahuje hypotetické scenáre, ktoré slúžia ako praktické príklady rôznych problémov, ktoré sa vyskytujú v tejto stále sa meniacej oblasti.

AGENTÚRA EURÓPSKEJ ÚNIE PRE ZÁKLADNÉ PRÁVA

Schwarzenbergplatz 11 – 1040 Viedeň – Rakúsko
Tel. +43 (1) 580 30-0 – Fax +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EURÓPSKY SÚD PRE ĽUDSKÉ PRÁVA RADA EURÓPY

67075 Štrasburg Cedex – Francúzsko
Tel. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

Rue Wiertz 60 – 1047 Brusel – Belgicko
Tel. +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS



Úrad pre vydávanie publikácií
Európskej únie

ISBN 978-92-871-9823-5 (Rada Európy)
ISBN 978-92-9461-307-3 (FRA)