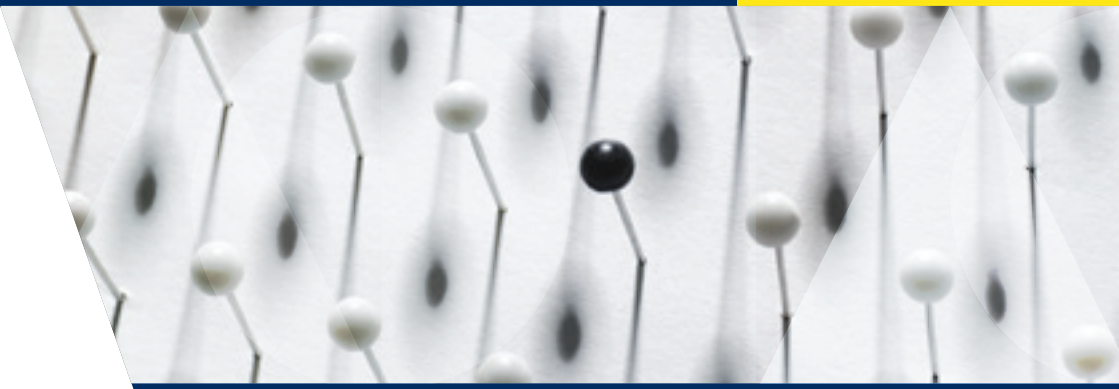
PRÍRUČKA



Príručka o európskom práve v oblasti ochrany údajov

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Rukopis tejto príručky bol dokončený v apríl 2014.
V budúcnosti budú k dispozícii aktualizácie príručky na webovej stránke agentúry FRA na adrese: fra.europa.eu, na webovej stránke Rady Európy na adrese: coe.int/dataprotection a na webovej stránke Európskeho súdu pre ľudské práva v ponuke Case-Law (Judikatúra) na adrese: echr.coe.int.

Europe Direct je služba, ktorá vám pomôže nájsť odpovede na vaše otázky o Európskej únii.

Bezplatné telefónne číslo (*):

00 800 6 7 8 9 10 11

(*) Za poskytnutie informácií sa neplatí, podobne ako za väčšinu hovorov (niektorí mobilní operátori, verejné telefónne automaty alebo hotely si však môžu účtovať poplatok).

Fotografia na obálke a vo vnútri: © iStockphoto

Viac doplňujúcich informácií o Európskej únii je k dispozícii na internete. Sú dostupné cez server Európa (http://europa.eu).

Katalogizačné údaje sa nachádzajú na konci tejto publikácie.

Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2014

ISBN 978-92-871-9937-9 (Rada Európy)
ISBN 978-92-9239-340-3 (FRA)
doi:10.2811/55893

Printed in Belgium

Vytlačené na papieri bielenom bez použitia elementárneho chlóru (ECF)

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Príručka o európskom práve v oblasti ochrany údajov

Predslov

Príručku o európskom práve v oblasti ochrany údajov spoločne pripravili Agentúra Európskej únie pre základné práva (FRA) a Rada Európy v spolupráci s kanceláriou Európskeho súdu pre ľudské práva. Ide o tretiu príručku z radu právnych príručiek, ktoré spoločne vypracovali FRA a Rada Európy. V marci 2011 bola uverejnená prvá príručka o európskom antidiskriminačnom práve a v júni 2013 príručka o európskom práve v oblasti azylu, hraníc a imigrácie.

Rozhodli sme sa, že budeme pokračovať v spolupráci a zameriame sa na mimoriadne aktuálny problém, ktorý sa nás všetkých každodenne dotýka – na ochranu osobných údajov. Európsky systém patrí k tým, ktoré zabezpečujú najrozsiahlejšiu ochranu v tejto oblasti. Vychádza z dohovoru Rady Európy č. 108, nástrojov Európskej únie (EÚ), ako aj z judikatúry Európskeho súdu pre ľudské práva (ESĽP) a Súdneho dvora Európskej únie (SDEÚ).

Cieľom príručky je zvýšiť informovanosť a zlepšiť poznatky o právnych predpisoch v oblasti ochrany údajov v členských štátoch Európskej únie a Rady Európy a slúžiť ako hlavný referenčný zdroj, na ktorý sa čitatelia môžu obracať. Je určená pre profesionálnych právnikov, ktorí sa nešpecializujú na tento odbor, sudcov, vnútroštátne orgány pre ochranu osobných údajov a ďalšie osoby, ktoré pôsobia v oblasti ochrany údajov.

Po nadobudnutí účinnosti Lisabonskej zmluvy v decembri 2009 sa Charta základných práv EÚ stala právne záväzným dokumentom a právo na ochranu osobných údajov vďaka tomu získalo štatút samostatného základného práva. Zásadný význam pre ochranu tohto základného práva má lepšie pochopenie dohovoru Rady Európy č. 108 a nástrojov EÚ, ktoré pripravili pôdu pre ochranu údajov v Európe, ako aj pochopenie judikatúry SDEÚ a ESĽP.

Radi by sme poďakovali Inštitútu ľudských práv Ludwiga Boltzmanmna za ich príspevok k napísania tejto príručky. Taktiež by sme radi vyjadrili vďaku kancelárii európskeho dozorného úradníka pre ochranu údajov za spätnú väzbu pri písaní príručky. Ďakujeme predovšetkým oddeleniu Európskej komisie pre ochranu údajov za pomoc pri príprave tejto príručky.

Philippe Boillat

generálny riaditeľ pre ľudské práva a právny štát Rada Európy

Morten Kjaerum

riaditeľ Agentúry Európskej únie pre základné práva

Obsah

Skratky

CCTV	Priemyselná televízia
Charta	Charta základných práv
CIS	Colný informačný systém
C-SIS	Centrálny Schengenský informačný systém
Dohovor č. 108	Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Rada Európy)
EDĽP	Európsky dohovor o ľudských právach
EDPS	Európsky dozorný úradník pre ochranu údajov
EHP	Európsky hospodársky priestor
ENISA	Európska agentúra pre bezpečnosť sietí a informácií
ES	Európske spoločenstvo
ESĽP	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 pre rozsiahle informačné systémy
EuroPriSe	Európske osvedčenie o zachovaní dôverného charakteru
EZVO	Európske združenie voľného obchodu
FRA	Agentúra Európskej únie pre základné práva
GPS	Globálny polohový systém
MVO	Mimovládna organizácia
N-SIS	Národný Schengenský informačný systém
OECD	Organizácia pre hospodársku spoluprácu a rozvoj
OSN	Organizácia Spojených národov
PIN	Osobné identifikačné číslo

PNR	Osobný záznam o cestujúcom
SDEÚ	Európsky súdny dvor (do decembra 2009 sa nazýval Súdny dvor Európskych spoločenstiev, SD)
SEPA	Jednotná oblasť platieb v eurách
SIS	Schengenský informačný systém
SWIFT	Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu
VIS	Vízový informačný systém
ZEÚ	Zmluva o Európskej únii
ZFEÚ	Zmluva o fungovaní Európskej únie

Ako používať túto príručku

Príručka obsahuje prehľad práva týkajúceho sa ochrany údajov v rámci Európskej únie (EÚ) a Rady Európy (RE).

Jej úlohou je pomôcť právnym zástupcom, ktorí sa nešpecializujú na oblasť ochrany údajov – je určená pre právnikov, sudcov alebo iných odborníkov, ako aj pre osoby pracujúce pre iné orgány vrátane mimovládnych organizácií (MVO), ktorí sa môžu stretávať s právnymi otázkami z oblasti ochrany údajov.

Predstavuje prvý referenčný zdroj pokiaľ ide o právo EÚ a Európsky dohovor o ľudských právach (EDĽP) v oblasti ochrany údajov a vysvetľuje sa v nej, ako je táto oblasť regulovaná podľa právnych predpisov EÚ a EDĽP, ako aj Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108) a ďalších nástrojov Rady Európy. V každej kapitole je najskôr uvedená samostatná tabuľka s platnými právnymi ustanoveniami vrátane dôležitej vybranej judikatúry v rámci dvoch samostatných európskych právnych systémov. Potom sú jeden po druhom predstavené príslušné právne predpisy oboch európskych právnych poriadkov, ktoré by sa mohli uplatniť na jednotlivé otázky. To umožní čitateľom uvidieť spoločné aj odlišné miesta oboch právnych systémov.

V tabuľkách v úvode jednotlivých kapitol sú vymenované témy, ktorým sú venované príslušné kapitoly, pričom sú sprevádzané relevantnými právnymi ustanoveniami a ďalším informáciami, napríklad judikatúrou. Poradie tém sa môže nepatrne líšiť od štruktúry textu v kapitole, ak je to vhodnejšie z hľadiska stručného predstavenia obsahu kapitoly. Tabuľky zahŕňajú právny poriadok Rady Európy aj EÚ. To by malo používateľom pomôcť nájsť hlavné informácie týkajúce sa ich situácie, predovšetkým vtedy, keď sa na nich vzťahujú len právne predpisy Rady Európy.

Právnici v štátoch mimo EÚ, ktoré sú členskými štátmi Rady Európy a zmluvnými stranami EDĽP a dohovoru č. 108, získajú prístup k informáciám relevantným pre príslušnú krajinu tak, že priamo prejdú na oddiely o Rade Európy. Právnici z členských štátov EÚ budú musieť použiť oba oddiely, keďže tieto štáty sú viazané obidvoma právnymi poriadkami. Pre tých, ktorí potrebujú viac informácií o konkrétnom probléme, je v oddiele príručky s názvom Doplňujúca literatúra uvedený zoznam odkazov na odbornejšie materiály.

Právo Rady Európy je predstavené prostredníctvom krátkych odkazov na vybrané prípady Európskeho súdu pre ľudské práva (ESĽP). Pochádzajú z veľkého množstva rozsudkov a rozhodnutí, ktoré ESĽP prijal v oblasti ochrany údajov.

Právo EÚ je vyjadrené prostredníctvom prijatých legislatívnych nástrojov, príslušných ustanoveniach zmlúv a Charty základných práv Európskej únie tak, ako ich vykladá judikatúra Súdneho dvora Európskej únie (SDEÚ) (do roku 2009 sa nazýval Súdny dvor Európskych spoločenstiev – SD).

V judikatúre opísanej alebo citovanej v tejto príručke sa uvádzajú príklady dôležitého korpusu judikatúry ESĽP aj SDEÚ. Usmernenia uvedené v závere príručky majú pomôcť čitateľom pri vyhľadávaní judikatúry on-line.

Okrem toho sú v textových poliach uvedené praktické názorné príklady s hypotetickými scenármi, ktoré 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.

Príručka sa začína stručným opisom úlohy dvoch právnych systémov stanovených EDĽP 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,
- práva dotknutých osôb a ich presadzovanie,
- cezhraničný tok údajov,
- ochrana údajov v kontexte polície a trestného súdnictva,
- ďalšie osobitné európske právne predpisy o ochrane údajov.

1

Kontext a východiská európskeho práva v oblasti ochrany údajov

EÚ	Zahrnuté témy	Rada Európy
Právo na ochranu údajov		
Smernica 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (*smernica o ochrane údajov*), Ú. v. ES L 281, 1995		EDĽP, článok 8 (právo na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie) Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108)
Vyváženie práv		
SDEÚ, Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen*, 2010	**Všeobecne**	
SDEÚ, C-73/07, *Tietosuojavaltuutettu/ Satakunnan Markkinapörssi Oy a Satamedia Oy*, 2008	**Sloboda prejavu**	ESĽP, *Axel Springer AG/ Nemecko*, 2012 ESĽP, *Mosley/Spojené kráľovstvo*, 2011
	Sloboda umenia a vedeckého bádania	ESĽP, *Vereinigung bildender Künstler/Rakúsko*, 2007
SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 2008	**Ochrana vlastníctva**	
SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd*, 2010	**Prístup k dokumentom**	ESĽP, *Társaság a Szabadságjogokért/ Maďarsko*, 2009

1.1. Právo na ochranu údajov

Hlavné body

- Podľa článku 8 EDĽP tvorí právo na ochranu pred zberom a používaním osobných údajov časť práva na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie.
- Dohovor Rady Európy č. 108 predstavuje prvý medzinárodný právne záväzný nástroj, v ktorom sa zaoberá výslovne ochranou údajov.
- V rámci právnych predpisov EÚ bola ochrana údajov prvýkrát regulovaná smernicou o ochrane údajov.
- V rámci právnych predpisov EÚ bola ochrana údajov uznaná ako základné právo.

Právo na ochranu súkromnej sféry jednotlivca pred zasahovaním zo strany iných subjektov, predovšetkým štátu, bolo v medzinárodnom právnom dokumente prvýkrát zakotvené v článku 12 Všeobecnej deklarácie ľudských práv OSN v roku 1948 a uvedený článok sa týkal rešpektovania súkromného a rodinného života[1]. Všeobecná deklarácia ľudských práv ovplyvnila vývoj ďalších nástrojov v oblasti ľudských práv v Európe.

1.1.1. 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. Rada Európy s týmto cieľom v roku 1950 schválila Európsky dohovor o ľudských právach, ktorý nadobudol účinnosť v roku 1953.

Štáty majú medzinárodnú povinnosť dodržiavať ustanovenia EDĽP. Všetky členské štáty Rady Európy začlenili EDĽP do svojich vnútroštátnych právnych predpisov alebo v ich rámci nadobudol účinnosť, a preto musia konať v zhode s ustanoveniami tohto dohovoru.

S cieľom zabezpečiť plnenie povinností vyplývajúcich z EDĽP pre zmluvné strany bol v Štrasburgu v roku 1959 zriadený Európsky súd pre ľudské práva (ESĽP). Úlohou súdu je zabezpečiť, aby štáty plnili záväzky vyplývajúce z dohovoru a zaoberali sa sťažnosťami jednotlivých osôb, skupín jednotlivcov, mimovládnych organizácií alebo

1 Organizácia Spojených národov, Všeobecná deklarácia ľudských práv (VDĽP), 10. Decembra 1948.

právnických osôb, ktoré sa sťažujú na údajné porušenie dohovoru. V roku 2013 mala Rada Európy 47 členských štátov, pričom 28 z nich bolo zároveň členskými štátmi EÚ. Sťažovateľ, ktorý sa obracia na ESĽP, nemusí byť štátnym príslušníkom členského štátu Rady Európy. ESĽP môže posudzovať takisto medzištátne spory vedené jedným členským štátom alebo niekoľkými členskými štátmi Rady Európy proti druhému členskému štátu.

Právo na ochranu osobných údajov tvorí časť práv chránených podľa článku 8 EDĽP, ktorým sa zaručuje právo na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie a stanovujú podmienky prípustnosti obmedzenia tohto práva[2].

ESĽP v rámci svojej judikatúry posudzoval veľa prípadov, ktoré sa týkali ochrany údajov, okrem iného prípady odpočúvania komunikácie[3], rôznych foriem sledovania[4] a ochrany pred uchovávaním osobných údajov verejnými orgánmi[5]. Vysvetlil, že z článku 8 EDĽP 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 zaisťovať účinné rešpektovanie súkromného a rodinného života[6]. Viacerými z týchto prípadov sa budeme zaoberať v príslušných kapitolách.

1.1.2. Dohovor Rady Európy č. 108

Vznik informačnej technológie v 60. rokoch 20. storočia priniesol čoraz naliehavejšiu potrebu prijať podrobné pravidlá ochrany jednotlivcov formou ochrany ich (osobných) údajov. V polovici 70. rokov prijal Výbor ministrov Rady Európy niekoľko uznesení o ochrane osobných údajov, v ktorých sa odkazovalo na článok 8 EDĽP[7]. V roku 1981 bol Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní

2 Rada Európy, Európsky dohovor o ľudských právach, Súbor dohovorov Rady Európy č. 005, 1950.

3 Pozri napríklad ESĽP, *Malone/Spojené kráľovstvo*, č. 8691/79, 2. augusta 1984; ESĽP, *Copland/Spojené kráľovstvo*, č. 62617/00, 3. apríla 2007.

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

5 Pozri napríklad ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987; ESĽP, *S. a Marper/Spojené kráľovstvo*, č. 30562/04 a 30566, 4. decembra 2008.

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

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

osobných údajov (dohovor č. 108)[8] 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 spracovanie osobných údajov v súkromnom ako aj verejnom sektore, ako napríklad spracovanie osobných údajov v súdnictve či orgánmi činnými v trestnom konaní. Chráni jednotlivca pred zneužitím, ktoré by mohlo sprevádzať zber a spracovanie osobných údajov, a zároveň sa ním má regulovať cezhraničný tok osobných údajov. Pokiaľ ide o zber a spracúvanie osobných údajov, zásady stanovené v dohovore sa týkajú predovšetkým spravodlivého a zákonného zberu a automatizovaného spracúvania údajov, ktoré sa uchovávajú na špecifikované legitímne účely a nepoužívajú sa na ciele nezlučiteľné s týmito účelmi, ani sa neuchovávajú dlhšie, než je to nevyhnutne potrebné. Uvedenými zásadami sa upravuje aj kvalita údajov, predovšetkým ich adekvátnosť a relevantnosť, ako aj to, že údaje nesmú byť nadbytočné (primeranosť) a musia byť presné.

Okrem poskytnutia záruk týkajúcich sa zberu a spracúvania osobných údajov sa dohovorom upravuje (ak neexistujú primerané právne záruky) spracúvanie tzv. citlivých údajov napríklad o rase, politických postojoch, zdravotnom stave, náboženskom presvedčení, sexuálnom živote či údajov z registra 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.

V dohovore sa síce umožňuje voľný tok osobných údajov medzi zmluvnými stranami (štátmi) dohovoru, zároveň sa v ňom však ukladajú určité obmedzenia tohto toku pre štáty, v ktorých právna úprava nezabezpečuje primeranú ochranu.

Výbor ministrov rady Európy prijal v záujme prehĺbenia všeobecných zásad a pravidiel stanovených v dohovore č. 108 niekoľko odporúčaní, ktoré nie sú právne záväzné (pozri kapitoly 7 a 8).

8 Rada Európy, Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, Rada Európy, Súbor dohovorov Rady Európy č. 108, 1981.

Dohovor č. 108 ratifikovali všetky členské štáty EÚ. V roku 1999 bol dohovor zmenený tak, aby umožnil EÚ stať sa zmluvnou stranou[9]. V roku 2001 bol prijatý dodatkový protokol k dohovoru č. 108, ktorým sa zavádzajú ustanovenia o cezhraničnom toku údajov pre strany, ktoré nie sú zmluvnými stranami dohovoru (tzv. tretie krajiny), ako aj ustanovenia o povinnom zriadení vnútroštátnych orgánov dozoru nad ochranou údajov[10].

Výhľad

Na základe rozhodnutia o modernizácii dohovoru č. 108 sa v roku 2011 uskutočnili verejné konzultácie, ktoré umožnili potvrdiť dva hlavné ciele tejto činnosti: posilnenie ochrany súkromia v digitálnej oblasti a upevnenie kontrolných mechanizmov dohovoru.

K dohovoru č. 108 môže pristúpiť aj štát, ktorý nie je členom Rady Európy vrátane mimoeurópskych štátov. Potenciál dohovoru ako všeobecnej normy a jeho otvorenosť by mohli slúžiť ako základ na podporu ochrany údajov na celosvetovej úrovni.

V súčasnosti je 45 zo 46 zmluvných strán dohovoru č. 108 členskými štátmi Rady Európy. Prvá mimoeurópska krajina – Uruguaj – pristúpila k dohovoru v roku 2013 a Maroko, ktoré na pristúpenie k dohovoru č. 108 vyzval Výbor ministrov, je vo fáze formalizácie pristúpenia.

1.1.3. Právne predpisy Európskej únie o ochrane údajov

Právne predpisy EÚ tvoria zmluvy a sekundárne právo EÚ. Zmluvy, predovšetkým Zmluva o Európskej únii (ZEÚ) a Zmluva o fungovaní Európskej únie (ZFEÚ), boli schválené všetkými členskými štátmi EÚ a nazývajú sa tiež „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“.

9 Rada Európy, dodatky k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (ETS č. 108) umožňujúce Európskym spoločenstvám pristúpiť k dohovoru, prijaté Výborom ministrov v Štrasburgu 15. júna 1999; čl. 23 ods. 2 dohovoru č. 108 v jeho zmenenej podobe.

10 Rada Európy, dodatkový protokol k Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov týkajúci sa orgánov dozoru a cezhraničných tokov údajov, Súbor dohovorov Rady Európy č. 181, 2001.

Hlavným právnym nástrojom Európskej únie v oblasti ochrany údajov je 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*)[11]. Bola prijatá v roku 1995, v čase, keď niektoré členské štáty už mali vnútroštátne právne predpisy o ochrane údajov. 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 spoľahnúť na jednotnú vysokú úroveň ochrany údajov.

Keďže cieľom prijatia smernice o ochrane údajov bola harmonizácia[12] právnych predpisov o ochrane údajov na vnútroštátnej úrovni, v smernici sa umožňuje určitá miera špecifickosti porovnateľná s vnútroštátnymi právnymi predpismi o ochrane údajov existujúcimi v čase jej prijatia. Podľa SDEÚ „smernica 95/46 má za cieľ [...] dosiahnuť v súvislosti so spracovávaním osobných údajov vo všetkých členských štátoch rovnakú úroveň ochrany práv a slobôd. [...] Aproximácia právnych predpisov v tejto oblasti nesmie mať za následok zníženie ochrany, ktorú poskytujú, ale naopak, musí mať za cieľ zabezpečenie vysokej úrovne ochrany v Únii. V tejto súvislosti [...] vyplýva, že harmonizácia týchto vnútroštátnych právnych predpisov sa neobmedzuje na minimálnu harmonizáciu, ale smeruje k takej harmonizácii, ktorá je v zásade úplná.“.[13] Členské štáty majú teda len obmedzenú voľnosť pri vykonávaní smernice.

Účelom smernice o ochrane údajov je zdôrazniť význam zásad práva na súkromie zahrnutých do dohovoru č. 108 a rozšíriť ich. Skutočnosť, že v roku 1995 bolo všetkých 15 členských štátov EÚ zároveň zmluvnými stranami dohovoru č. 108, vylúčila prijatie protirečivých ustanovení v uvedených dvoch právnych nástrojoch. V smernici o ochrane údajov sa však využíva možnosť rozšírenia nástrojov na ochranu stanovenú v článku 11 dohovoru č. 108. Ukázalo sa, že dôležitým príspevkom k efektívnemu fungovaniu európskych právnych predpisov o ochrane údajov bolo najmä zavedenie nezávislého dohľadu ako nástroja na zlepšenie súladu s týmito predpismi. (Funkcia dohľadu bola v roku 2001 následne prevzatá do právnych predpisov Rady Európy prijatím dodatkového protokolu k dohovoru č. 108.)

11 Smernica o ochrane údajov, Ú. v. ES L 281, 1995, s. 31.

12 Pozri napríklad smernicu o ochrane údajov, odôvodnenia 1, 4, 7 a 8.

13 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, body 28-29.

Územné uplatňovanie smernice o ochrane údajov prekračuje hranice 28 členských štátov EÚ a zahŕňa aj štáty, ktoré nie sú členskými štátmi EÚ, ale patria do Európskeho hospodárskeho priestoru (EHP)[14], a to Island, Lichtenštajnsko a Nórsko.

Právomoc určovať, či členský štát plní svoje povinnosti vyplývajúce zo smernice o ochrane údajov a vynášať predbežné rozsudky týkajúce sa platnosti a interpretácie smernice má SDEÚ v Luxemburgu s cieľom zaistiť účinné a jednotné uplatňovanie smernice v členských štátoch. Dôležitou výnimkou z uplatňovania smernice o ochrane údajov je tzv. výnimka pre domáce činnosti, konkrétne pre spracúvanie osobných údajov súkromnými osobami na výlučne osobné účely alebo účely domácnosti[15]. Takéto spracúvanie sa vo všeobecnosti pokladá za súčasť slobôd súkromnej osoby.

V súlade s primárnym právom platným v čase prijatia smernice o ochrane údajov je vecný rozsah smernice obmedzený na záležitosti vnútorného trhu. Mimo rozsahu jej pôsobnosti sa nachádzajú predovšetkým záležitosti spolupráce v oblasti polície a trestného súdnictva. Ochrana údajov v tejto oblasti vyplýva z rôznych právnych nástrojov, ktoré sú podrobne opísané v kapitole 7.

Keďže smernica o ochrane údajov je určená len pre členské štáty EÚ, bolo potrebné prijať ďalší právny nástroj s cieľom stanoviť ochranu údajov pri spracovaní 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 pri spracovaní údajov inštitúciami EÚ*)[16].

Dokonca aj v oblastiach zahrnutých do smernice o ochrane údajov sú často potrebné podrobnejšie ustanovenia o ochrane údajov v záujme dosiahnutia nevyhnutne potrebnej jasnosti pri vyvážení ďalších oprávnených záujmov. Ako dva príklady poslúžia smernica 2002/58/ES, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (*smernica o súkromí*

14 Dohoda o Európskom hospodárskom priestore, Ú. v. ES L 1, 1994, ktorá nadobudla účinnosť 1. Januára 1994.

15 Smernica o ochrane údajov, článok 3 ods. 2 druhá zarážka.

16 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.

a elektronických komunikáciách)[17] a smernica 2006/24/ES 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/EC (*smernica o uchovávaní údajov*, ktorá bola vyhlásená za neplatnú 8. apríla 2014)[18]. Ďalšie príklady uvedieme v kapitole 8. Takéto ustanovenia musia byť v súlade so smernicou o ochrane údajov.

Charta základných práv Európskej únie

Pôvodné zmluvy o založení Európskych spoločenstiev neobsahujú žiadne odkazy na ľudské práva alebo ich ochranu. Keď sa však pred vtedajší Súdny dvor Európskych spoločenstiev (SD) dostali prípady údajného porušenia ľudských práv v oblastiach, ktoré patrili do rozsahu pôsobnosti právnych predpisov EÚ, zaujal sa nový prístup. V záujme poskytnutia ochrany jednotlivcom boli základné práva zahrnuté do tzv. všeobecných zásad európskeho práva. Podľa SDEÚ tieto všeobecné zásady odrážajú obsah ochrany ľudských práv zakotvenej v ústavách jednotlivých členských štátov a zmluvách o ochrane ľudských práv, a najmä v EDĽP. SDEÚ konštatoval, že sa tak zaistí 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 „bližšie" EÚ, v roku 2000 vyhlásila Chartu základných práv Európskej únie (charta). Charta zahŕňa celý súbor občianskych, politických, hospodárskych a sociálnych práv európskych občanov, a to tak, že sa v nej spájajú ústavné tradície a medzinárodné záväzky spoločné pre členské štáty. Práva opísané v charte sú rozdelené do šiestich oddielov: dôstojnosť, sloboda, rovnosť, solidarita, občianstvo a spravodlivosť.

Charta bola pôvodne len politickým dokumentom, ale po nadobudnutí účinnosti Lisabonskej zmluvy 1. decembra 2009[19] sa stala právne záväznou[20] ako primárne právo EÚ (pozri článok 6 ods. 1 ZEÚ).

17 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.

18 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, *(smernica o uchovávaní údajov),* Ú. v. EÚ L 105, 2006, ktorá bola vyhlásená za neplatnú 8. apríla 2014.

19 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.

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

Primárne právo EÚ takisto zahŕňa všeobecnú právomoc EÚ prijímať právne predpisy v oblasti ochrany údajov (článok 16 ZFEÚ).

V charte sa nielen zaručuje rešpektovanie súkromného a rodinného života (článok 7), ale stanovuje aj právo na ochranu údajov (článok 8), pričom sa v nej výslovne zvyšuje úroveň ochrany na úroveň prislúchajúcu ochrane základného práva v rámci právnych predpisov EÚ. Inštitúcie, ako aj členské štáty EÚ, musia toto právo dodržiavať a zaručovať. 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 text začleňujúci predchádzajúce 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). Článkom 8 ods. 3 charty sa zaručuje kontrola vykonávania uvedených zásad nezávislým orgánom.

Výhľad

V januári 2012 Európska komisia predložila reformný balík právnych predpisov o ochrane údajov, v ktorom sa uvádza, že vzhľadom na prudký vývoj technológií a globalizáciu je potrebné modernizovať platné pravidlá ochrany údajov. Reformný balík tvorí návrh všeobecného nariadenia o ochrane údajov[21], ktorý má nahradiť smernicu o ochrane údajov, ako aj nová smernica o ochrane údajov[22], ktorou sa zaručuje ochrana údajov v oblastiach politickej a súdnej spolupráce v trestných veciach. V čase uverejnenia tejto príručky prebiehala diskusia o reformnom balíku.

1.2. Vyváženie práv

Hlavný bod

- Právo na ochranu údajov nie je absolútne právo. Musí byť vyvážené s ostatnými právami.

21 Európska komisia (2012), *Návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov)*, KOM(2012) 11 v konečnom znení, Brusel, 25. januára 2012.

22 Európska komisia (2012), *Návrh smernica Európskeho parlamentu a Rady 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 všeobecnej ochrane údajov)*, KOM(2012) 10 v konečnom znení, Brusel, 25. januára 2012.

Základné právo na ochranu osobných údajov podľa článku 8 charty „sa však nejaví ako absolútne právo, ale musí sa zohľadniť so zreteľom na jeho funkciu v spoločnosti“[23]. V článku 52 ods. 1 charty sa teda prijíma skutočnosť, že výkon práv je možné obmedziť napríklad obmedzeniami stanovenými v článkoch 7 a 8 charty, ak sú takéto obmedzenia stanovené zákonom, rešpektujú podstatu daných práv a slobôd a podľa zásady proporcionality sú nevyhnutné a skutočne zodpovedajú cieľom všeobecného záujmu uznaným Európskou úniou alebo potrebe ochrany práv a slobôd iných[24].

V systéme EDĽP je ochrana údajov zaručená článkom 8 (právo na rešpektovanie súkromného a rodinného života) a podobne ako v systéme charty sa toto právo musí uplatňovať tak, aby sa rešpektoval rozsah pôsobnosti ďalších konkurenčných práv. Podľa článku 8 ods. 2 EDĽP „štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti [...] na ochranu práv a slobôd iných“.

ESĽP aj SDEÚ teda opakovane konštatovali, že pri uplatňovaní a výklade článku 8 EDĽP a článku 8 charty je nutné vyvážiť vykonávanie s ostatnými právami[25]. Ukážeme si na niekoľkých príkladoch, ako sa takáto rovnováha dosahuje.

1.2.1. Sloboda prejavu

Jedným z práv, pri ktorom je pravdepodobný konflikt s právom na ochranu údajov, 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“. Článok 11 charty zodpovedá článku 10 EDĽP. Podľa článku 52 ods. 3 charty, v rozsahu, v akom obsahuje práva, ktoré zodpovedajú právam zaručeným v EDĽP,

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

24 Tamtiež, bod 50.

25 ESĽP, *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 (FECEMD)/Administración del Estado*, 24. novembra 2011, bod. 48; SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 29. januára 2008, bod 68. Pozri takisto Rada Európy (2013), judikatúra Európskeho súdu pre ľudské práva týkajúca sa ochrany osobných údajov, judikatúra DP (2013), dostupné na adrese: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf

„zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom dohovore“. Obmedzenia, ktoré môžu byť zo zákona uložené na právo zaručené článkom 11 charty, teda nesmú byť rozsiahlejšie, ako obmedzenia stanovené v článku 10 ods. 2 EDĽP, čo znamená, že musia byť predpísané zákonom a musia byť nutné v demokratickej spoločnosti „na ochranu [...] povesti alebo práv iných“. Táto koncepcia zahŕňa právo na ochranu údajov.

Vzťah medzi ochranou osobných údajov a slobodou prejavu je upravený článkom 9 smernice o ochrane údajov s názvom Spracovanie osobných údajov a sloboda prejavu[26]. Podľa tohto článku 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.

Príklad: SDEÚ bol vo veci *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy*[27] požiadaný o výklad článku 9 smernice o ochrane údajov a vymedzenie vzťahu medzi ochranou údajov a slobodou tlače. Súd preskúmal šírenie údajov o daniach približne 1,2 milióna fyzických osôb v novinách Markkinapörssi a Satamedia, pričom uvedené údaje boli zákonným spôsobom získané od fínskych daňových orgánov. Súd musel predovšetkým overiť, či sa spracovanie osobných údajov, ktoré daňové orgány sprístupnili s cieľom umožniť používateľom mobilných telefónov získať údaje o daniach týkajúce sa iných fyzických osôb, musí pokladať za činnosť vykonávanú výlučne na žurnalistické účely. Súd dospel k záveru, že činnosť spoločnosti Satakunnan predstavovala „spracúvanie osobných údajov“ v zmysle článku 3 ods. 1 smernice o ochrane údajov a pokračoval výkladom článku 9 uvedenej smernice. Najskôr poukázal na význam práva na slobodu prejavu v každej demokratickej spoločnosti a uviedol, že 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 súd dospel k záveru, že činnosti spoločnosti Markkinapörssi a Satamedia týkajúce sa údajov z dokumentov, ktoré sú podľa vnútroštátnych právnych predpisov verejné, možno klasifikovať ako „žurnalistické

26 Smernica o ochrane údajov, článok 9.

27 SDEÚ, C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy*, 16. Decembra 2008, body 56, 61 a 62.

činnosti“ vtedy, keď je ich cieľom zverejnenie informácií, názorov alebo myšlienok bez ohľadu na médium použité na ich prenos. Súd sa takisto uzniesol, že tieto činnosti nie sú obmedzené na mediálne podniky a môžu sa vykonávať na účely vytvorenia zisku. Rozhodnutie o tom, či sa to týka aj tohto konkrétneho prípadu, však ponechal na vnútroštátnom súde.

ESĽP vyniesol niekoľko prelomových rozsudkov, pokiaľ ide o zosúladenie práva na ochranu údajov s právom na slobodu prejavu.

Príklad: V rozsudku *Axel Springer AG/Nemecko*[28] ESĽP dospel k záveru, že zákaz vydaný vnútroštátnym súdom pre majiteľa novín, ktorý chcel uverejniť článok o uväznení a odsúdení známeho herca, predstavuje porušenie článku 10 EDĽP. ESĽP pripomenul kritériá, ktoré stanovil vo svojej judikatúre, pokiaľ ide o vyváženie práva na slobodu prejavu s právom na rešpektovanie súkromného života:

- po prvé, či udalosť, ktorej sa týkal uverejnený článok, bola vo všeobecnom záujme: uväznenie a odsúdenie osoby predstavovalo verejnú súdnu skutočnosť, išlo teda o verejný záujem;
- po druhé, či dotknutá osoba bola verejnou osobou: dotknutou osobou bol herec dostatočne známy na to, aby sa mohol považovať za verejnú osobu;
- po tretie, akým spôsobom boli informácie získané a či boli spoľahlivé: informácie poskytla kancelária prokurátora a strany nespochybnili presnosť informácií uvedených v oboch prípadoch uverejnenia.

ESĽP sa teda uzniesol, že zákaz uverejnenia uložený spoločnosti nebol primeraný legitímnemu cieľu ochrany súkromného života sťažovateľa. Súd dospel k záveru, že došlo k porušeniu článku 10 EDĽP.

Príklad: Vo veci *Von Hannover/Nemecko (č. 2)*[29] ESĽP nezistil žiadne porušenie práva na rešpektovanie súkromného života vyplývajúceho z článku 8 EDĽP v zamietnutí žiadosti monackej princeznej Caroline o zákaz zverejnenia fotografie princeznej a jej manžela na lyžiarskej dovolenke. Fotografiu sprevádzal článok, ktorý okrem iného referoval o zlom zdravotnom stave kniežaťa Rainiera. ESĽP dospel k záveru, že vnútroštátne súdy dôkladne vyvážili právo

28 ESĽP, *Axel Springer AG/Nemecko*, [VK], č. 39954/08, 7. Februára 2012, body 90 a 91.

29 ESĽP, *Von Hannover/Nemecku (č. 2)* [VK], č. 40660/08 a 60641/08, 7. februára 2012, body 118 a 124.

spravodajských spoločností na slobodu prejavu s právom sťažovateľov na rešpektovanie ich súkromného života. Charakteristiku ochorenia kniežaťa Rainiera ako udalosti v súčasnej spoločnosti, ktorú predložili vnútroštátne súdy, nemožno pokladať za neodôvodnenú a ESĽP mohol súhlasiť s tým, že fotografia posudzovaná so zreteľom na článok prispela aspoň do určitej miery do diskusie vo všeobecnom záujme. Súd dospel k záveru, že nedošlo k porušeniu článku 8 EDĽP.

Jedným zo zásadných kritérií judikatúry ESĽP týkajúcich sa vyváženia uvedených práv je, či predmetný prejav prispieva alebo neprispieva k diskusii vo všeobecnom verejnom záujme.

Príklad: Vo veci *Mosley/Spojené kráľovstvo*[30] celoštátny týždenník uverejnil intímne fotografie sťažovateľa. Sťažovateľ sa následne sťažoval na údajné porušenie článku 8 EDĽP, keďže nemohol požadovať vydanie súdneho príkazu pred uverejnením predmetných fotografií z dôvodu neexistencie požiadavky, aby noviny vopred oznámili uverejnenie materiálu, ktorý by mohol porušovať právo jednotlivca na súkromie. Aj keď účelom šírenia takéhoto materiálu nebolo vzdelávanie, ale vo všeobecnosti skôr zábava, nepochybne sa naň vzťahuje ochrana vyplývajúca z článku 10 EDĽP, ktorý sa môže oprieť o požiadavky článku 8 EDĽP v prípadoch súkromnej a intímnej povahy informácií, keď neexistuje žiadny verejný záujem na ich šírení. Zvlášť opatrne treba postupovať pri skúmaní prekážok, ktoré by mohli fungovať ako forma cenzúry pred uverejnením. Pokiaľ ide o „zmrazenie", ktoré by mohlo byť dôsledkom požiadavky na predbežné oznamovanie, o pochybnosti o účinnosti takejto požiadavky a široký rozsah uznania v tejto oblasti, ESĽP dospel k záveru, že z článku 8 nevyplýva povinnosť existencie právne záväznej požiadavky na predbežné oznamovanie. Následne súd konštatoval, že nedošlo k porušeniu článku 8.

Príklad: Vo veci *Biriuk/ Litva*[31] si sťažovateľka nárokuje odškodné od denníka, ktorý uverejnil článok s informáciami o tom, že sťažovateľka je HIV pozitívna. Tieto informácie údajne potvrdili zdravotníci v miestnej nemocnici. ESĽP sa nedomnieval, že predmetný článok prispel k nejakej diskusii vo všeobecnom záujme a znova pripomenul, že ochrana osobných údajov, a najmä zdravotných údajov, má zásadný význam pre uplatnenie práva jednotlivca na rešpektovanie súkromia a rodinného života vyplývajúceho z článku 8 EDĽP. Súd osobitne

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

31 ESĽP, *Biriuk/Litva*, č. 23373/03, 25. novembra 2008.

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. Z toho vyplýva, že štát nedokázal ochrániť právo sťažovateľky na rešpektovanie jej súkromného života. Súd dospel k záveru, že došlo k porušeniu článku 8.

1.2.2. Prístup k dokumentom

Slobodný prístup k informáciám podľa článku 11 charty a článku 10 EDĽP chráni právo nielen na šírenie, ale aj na *prijímanie* informácií. Stále jasnejšie sa ukazuje význam transparentnosti štátnej správy pre fungovanie demokratickej spoločnosti. V uplynulých dvoch desaťročiach bol uznaný význam práva na prístup k dokumentom uchovávaným verejnými orgánmi ako dôležitého práva každého občana EÚ a každej fyzickej alebo právnickej osoby, ktorá má pobyt alebo sídlo v niektorom členskom štáte.

V rámci právnych predpisov Rady Európy sa 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*)[32]. **V rámci právnych predpisov EÚ** je právo prístupu k dokumentom zaručené nariadením č. 1049/2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (*nariadenie o prístupe k dokumentom*)[33]. 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". V súlade s článkom 52 ods. 2 charty sa právo prístupu k dokumentom takisto vykonáva za podmienok a v medziach určených v ustanoveniach článku 15 ods. 3 ZFEÚ. Toto právo by sa mohlo dostať do konfliktu s právom na ochranu údajov v prípade, keby sa sprístupnením dokumentov zverejnili osobné údaje iných osôb. 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: Vo veci *Komisia/Bavarian Lager*[34] SDEÚ vymedzil rozsah ochrany osobných údajov v kontexte prístupu k dokumentom inštitúcií EÚ a vzťah medzi

32 Rada Európy, Výbor ministrov (2002), odporúčanie Rec(2002)2 členským štátom o prístupe k oficiálnym dokumentom, 21. februára 2002; Rada Európy, Dohovor o prístupe k úradným dokumentom, Súbor dohovorov Rady Európy č. 205, 18. júna 2009. Dohovor zatiaľ nenadobudol účinnosť.

33 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.

34 SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd.*, 29. júna 2010, body 60, 63, 76, 78 a 79.

nariadeniami č. 1049/2001 (*nariadenie o prístupe k dokumentom*) a č. 45/2001 (*nariadenie o ochrane údajov*). 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 zosúladeniu 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 zamazala 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. Spoločnosť Bavarian Lager toto stanovisko neuspokojilo a podala žalobu na Súd prvého stupňa, ktorý anuloval rozhodnutie Komisie rozsudkom z 8. novembra 2007 (vec T-194/04, *Bavarian Lager/Komisia*), pričom zohľadnil skutočnosť, že uvedenie mien dotknutých osôb v zozname osôb, ktoré sa stretnutia 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 v celom ich rozsahu. SDEÚ následne dospel k záveru, že Komisia oprávnene zamietla žiadosť o prístup k celej zápisnici z októbra 1996. Keďže Komisia nezískala súhlas piatich účastníkov tohto stretnutia, svoju povinnosť otvorenosti dostatočne splnila tým, že zverejnila verziu predmetného dokumentu so zamazanými 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.

Podľa tohto rozsudku sa v prípadoch, keď právo na prístup k dokumentom zasahuje do práva na ochranu údajov, vyžaduje konkrétny a oprávnený dôvod. Právo prístupu k dokumentom nemôže automaticky zrušiť právo na ochranu údajov[35].

Nasledujúci rozsudok ESĽP sa zaoberá konkrétnym aspektom žiadosti o prístup.

Príklad: Vo veci *Társaság a Szabadságjogokért/Maďarsko*[36] požadoval sťažovateľ – mimovládna organizácia na ochranu ľudských práv – od Ústavného súdu prístup k informáciám o neuzatvorenej veci. Ústavný súd sa neobrátil na poslanca parlamentu, ktorý vec predložil, a odmietol žiadosť o prístup s odôvodnením, že sťažnosti, ktoré rieši, je možné sprístupniť tretím osobám len so súhlasom sťažovateľa. Vnútroštátne súdy potvrdili toto zamietnutie s odôvodnením, že ochrana osobných údajov nemôže byť prevýšená inými zákonnými záujmami vrátane dostupnosti verejných informácií. Sťažovateľ konal ako „strážny pes spoločnosti", ktorého činnosť má nárok na podobnú ochranu, akú má tlač. Pokiaľ ide o slobodu tlače, ESĽP sústavne potvrdzuje, že verejnosť má právo na informácie vo všeobecnom záujme. Informácie, ktoré požadovať sťažovateľ, boli „pripravené a k dispozícii" a nevyžadovali si žiadny zber údajov. Za takýchto okolností bol štát povinný nebrániť toku informácií, o ktoré žiadal sťažovateľ. ESĽP sa domnieval, že prekážky, ktoré majú zabrániť prístupu k informáciám vo verejnom záujme, by mohli odradiť pracovníkov v médiách alebo súvisiacich oblastiach od plnenia ich hlavnej úlohy „strážnych psov verejnosti". Súd dospel k záveru, že došlo k porušeniu článku 10.

V právnych predpisoch EÚ je dôrazne vyjadrený význam transparentnosti. Zásada transparentnosti je zakotvená v článkoch 1 a 10 ZEÚ a v článku 15 ods. 1 ZFEÚ[37]. Podľa odôvodnenia 2 nariadenia (ES) č. 1049/2001 transparentnosť umožňuje

35 Pozri napríklad podrobné rokovania na úrade Európskeho dozorného úradníka pre ochranu údajov (EDPS) (2011), *Verejný prístup k dokumentom obsahujúcim osobné údaje po vynesení rozsudku* Bavarian Lager**,** Brusel**,** 24. marca 2011, dostupné na adrese: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ESĽP, *Társaság a Szabadságjogokért/Maďarsko*, č. 37374/05, 14. apríla 2009; pozri body 27, 36–38.

37 EÚ (2012), Konsolidované verzie Zmluvy o Európskej únii a ZFEÚ, Ú. v. EÚ C 326, 2012.

občanom tesnejšie sa zapájať do rozhodovacieho procesu a zaručuje, že v demokratickom systéme sa administratíva stáva legitímnejšou, efektívnejšou a zodpovednejšou voči občanovi[38]. Na základe tohto odôvodnenia sa v nariadení Rady (ES) č. 1290/2005 o financovaní spoločnej poľnohospodárskej politiky a nariadení Komisie (ES) č. 259/2008, ktorým sa stanovujú podrobné pravidlá jeho uplatňovania, požaduje uverejňovanie informácií o príjemcoch pomoci z určitých fondov EÚ v sektore poľnohospodárstva a sumách, ktoré jednotliví príjemcovia prijali[39]. Uverejňovanie by malo prispievať k verejnej kontrole riadneho používania verejných financií štátnou správou. Primeranosť uverejnenia spochybnilo niekoľko príjemcov.

Príklad: SDEÚ musel vo veci *Volker a Markus Schecke a Hartmut Eifert/Land Hessen*[40] rozhodnúť o primeranosti uverejnenia mien príjemcov poľnohospodárskych dotácií EÚ a prijatých súm, ktoré sa požadovalo v právnych predpisoch EÚ.

Súdny dvor poznamenal, že právo na ochranu údajov nie je absolútne a argumentoval tým, že uverejnenie údajov s menami príjemcov z dvoch fondov poľnohospodárskej pomoci EÚ a presných súm, ktoré prijali, na webovej lokalite vo všeobecnosti predstavuje zásah do ich súkromného života, a konkrétne zásah do ochrany ich osobných údajov.

Súdny dvor zvážil, že takého porušenie článkov 7 a 8 charty bolo stanovené zákonom a dosiahlo cieľ všeobecného záujmu uznaný EÚ, a to vrátane zvýšenia transparentnosti používania financií Spoločenstva. Na druhej strane však potvrdil, že uverejnenie mien fyzických osôb, ktoré sú príjemcami poľnohospodárskej pomoci z uvedených dvoch fondov, a presných prijatých súm predstavuje neprimerané opatrenie, ktoré nie je oprávnené so zreteľom na článok 52 ods. 1 charty. Súdny dvor tak vyhlásil čiastočnú neplatnosť právnych predpisov EÚ o uverejňovaní informácií týkajúcich sa príjemcov pomoci z európskych poľnohospodárskych fondov.

38 SDEÚ, C-41/00 P, *Interporc Im- und Export GmbH/Komisia Európskych spoločenstiev*, 6. marca 2003, bod 39; SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd.*, 29. júna 2010, body 54.

39 Nariadenie Rady (ES) č. 1290/2005 z 21. júna 2005 o financovaní spoločnej poľnohospodárskej politiky, Ú. v. EÚ L 209, 2005 a 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 prijímateľoch pomoci zo zdrojov Európskeho poľnohospodárskeho záručného fondu (EPZF) a Európskeho poľnohospodárskeho fondu pre rozvoj vidieka (EPFRV), Ú. v. EÚ L 76, 2008.

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

1.2.3. Sloboda umenia a vedeckého bádania

Ďalším právom, ktoré je potrebné vyvážiť vzhľadom na právo na rešpektovanie súkromného života a ochranu údajov, je sloboda umenia a vedeckého bádania, ktorá je výslovne chránená na základe článku 13 charty. 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 EDĽP[41]. Aj na právo zaručené článkom 13 sa môžu vzťahovať obmedzenia vyplývajúce z článku 10 EDĽP[42].

Príklad: Vo veci *Vereinigung bildender Künstler/Rakúsko*[43] rakúske súdy zakázali združeniu sťažovateľa, aby vystavovalo obraz, ktorý obsahoval fotografie hláv rôznych verejne známych osôb 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 vyhovel jeho žiadosti a vydal súdny príkaz. ESĽP pripomenul, že článok 10 EDĽP sa uplatňuje na šírenie myšlienok, ktoré urážajú, poburujú alebo narušujú štát či niektorú časť obyvateľov. Osoby, ktoré vytvorili, predviedli, šírili 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, na ktorej boli použité iba hlavy osôb a ich telá boli namaľované nereálne a zveličené tak, že obraz zjavne nemal odrážať či dokonca naznačovať realitu, ESĽP 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“. ESĽP zvážil rôzne dotknuté záujmy a konštatoval, že neobmedzený zákaz ďalšieho vystavovania obrazu bol neprimeraný. Súd dospel k záveru, že došlo k porušeniu článku 10 EDĽP.

Pokiaľ ide o vedecké bádanie, v európskych právnych predpisoch o ochrane údajov je zohľadnená osobitná cena vedeckého bádania pre spoločnosť. Preto sú všeobecné obmedzenia používania osobných údajov zmiernené. Smernicou o ochrane údajov a dohovorom č. 108 sa povoľuje uchovávanie údajov na účely vedeckého výskumu

41 ESĽP, *Müller a iní/Švajčiarsko*, č. 10737/84, 24. mája 1988.

42 Vysvetlivky k Charte základných práv, Ú. v. EÚ C 303, 2007.

43 ESĽP, *Vereinigung bildender Künstler/Rakúsko*, č. 68345/01, 25. januára 2007; pozri predovšetkým body 26 a 34.

vtedy, keď údaje prestanú byť potrebné na počiatočný účel, na ktorý boli zozbierané. Následné použitie osobných údajov pri vedeckom výskume sa nepovažuje za nezlučiteľný účel. Podrobnejšie ustanovenia vrátane nevyhnutne potrebných záruk majú byť rozpracované vo vnútroštátnych právnych predpisoch s cieľom zosúladiť záujmy vedeckého výskumu s právom na ochranu údajov (pozri takisto oddiely 3.3.3 a 8.4).

1.2.4. Ochrana majetku

Právo na ochranu majetku je zakotvené v článku 1 prvého protokolu k EDĽP a tiež v článku 17 ods. 1 charty. Jedným z dôležitých aspektov práva na ochranu majetku je ochrana duševného vlastníctva, výslovne uvedená v článku 17 ods. 2 charty. V právnom poriadku EÚ je možné nájsť niekoľko smerníc zameraných na efektívnu ochranu duševného vlastníctva, predovšetkým autorských práv. Duševné vlastníctvo zahŕňa nielen literárne a umelecké vlastníctvo, ale aj patenty, ochranné známky a súvisiace práva.

Ako jasne vyplýva z judikatúry SDEÚ, ochrana základného práva na majetok musí byť vyvážená s ochranou ostatných základných práv, a najmä s právom na ochranu údajov[44]. Vyskytli sa prípady, v ktorých inštitúcie na ochranu autorských práv požadovali, aby poskytovatelia internetového pripojenia zverejnili totožnosť používateľov platforiem na zdieľanie súborov. Takéto platformy často umožňujú internetovým používateľom, aby si bezplatne preberali hudobné skladby, aj keď sú chránené autorským právom.

Príklad: Vec *Promusicae/Telefónica de España*[45] 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 občianskoprávne 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.

44 ESĽP, *Ashby Donald a iní/Francúzsko,* č. 36769/08, 10. januára 2013.

45 SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 29. januára 2008, body 54 a 60.

Španielsky súd postúpil vec SDEÚ a položil otázku, či takéto osobné údaje musia byť podľa práva Spoločenstva oznámené v kontexte občianskoprávneho sporu s cieľom zaistiť efektívnu ochranu autorských práv. Odkázal na smernice 2000/31, 2001/29 a 2004/48 v zmysle článkov 17 a 47 charty. Súdny dvor dospel k názoru, že v týchto troch smerniciach, ako aj v smernici o súkromí v 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 z tejto veci vyplynula otázka potreby zosúladenia požiadaviek ochrany rôznych základných práv, predovšetkým práva na rešpektovanie súkromného života, s právami na ochranu vlastníctva a účinného nápravného prostriedku.

Sú 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 súdy členských štátov pri vykonávaní opatrení na prebratie týchto smerníc nielen vykladali svoje vnútroštátne právo v súlade s uvedenými smernicami, 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 proporcionality...“[46].

46 Tamtiež, body 65 a 68; pozri tiež SDEÚ, C-360/10, *SABAM/Netlog NV*, 16. februára 2012.

2

Terminológia v oblasti ochrany údajov

EÚ	Zahrnuté otázky	Rada Európy
Osobné údaje		
Smernica o ochrane údajov, článok 2 písm. a) SDEÚ, Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen*, 9. novembra 2010 SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 29. januára 2008	Právne vymedzenie pojmu	Dohovor č. 108, článok 2 písm. a) ESĽP, *Bernh Larsen Holding AS a iní/Nórsko*, č. 24117/08, 14. marca 2013
Smernica o ochrane údajov, článok 8 ods. 1 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003	Osobitné kategórie osobných údajov (citlivé údaje)	Dohovor č. 108, článok 6
Smernica o ochrane údajov, článok 6 ods. 1 písm. e)	Anonymizované a pseudonymizované údaje	Dohovor č. 108, článok 5 písm. e) Dohovor č. 108, vysvetľujúca správa, článok 42
Spracúvanie údajov		
Smernica o ochrane údajov, článok 2 písm. b) SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003	Vymedzenia pojmov	Dohovor č. 108, článok 2 písm. c)
Používatelia údajov		
Smernica o ochrane údajov, článok 2 písm. d)	Prevádzkovateľ	Dohovor č. 108, článok 2 písm. d) Odporúčanie o profilovaní, článok 1 písm. g)*

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov, článok 2 písm. e) SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003	**Sprostredkovateľ**	Odporúčanie o profilovaní, článok 1 písm. h)
Smernica o ochrane údajov, článok 2 písm. g)	**Príjemca**	Dohovor č. 108, dodatkový protokol, článok 2 ods. 1
Smernica o ochrane údajov, článok 2 písm. f)	**Tretia strana**	
Súhlas		
Smernica o ochrane údajov, článok 2 písm. h) SDEÚ, C-543/09, *Deutsche Telekom AG/ Bundesrepublik Deutschland*, 5. mája 2011	**Vymedzenie platného súhlasu a požiadavky naň**	Odporúčanie o zdravotných údajoch, článok 6 a rôzne následné odporúčania

*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 súvisia s identifikovanou alebo aspoň identifikovateľnou osobou – dotknutou osobou.
- Osoba je identifikovateľná vtedy, keď je bez vynaloženia neprimeraného úsilia možné získať doplňujúce informácie umožňujúce identifikáciu dotknutej osoby.
- Autentifikácia znamená poskytnutie dôkazu o tom, že určitá osoba má určitú totožnosť a/alebo je oprávnená vykonávať určité činnosti.
- Existujú špeciálne kategórie údajov, tzv. citlivé údaje, ktoré sú uvedené v dohovore č. 108 a v smernici o ochrane údajov a ktoré si vyžadujú zvýšenú ochranu, preto sa na ne vzťahuje osobitný právny režim.
- Údaje sú anonymizované vtedy, keď už neobsahujú žiadne identifikačné znaky. Údaje sú pseudonymizované vtedy, keď sú identifikačné znaky zakódované.
- Pseudonymizované údaje sú na rozdiel od anonymizovaných údajov osobnými údajmi.

2.1.1. Hlavné aspekty pojmu osobných údajov

V rámci právnych predpisov EÚ, ako aj **právnych predpisov Rady Európy**, „osobné údaje“ sa definujú ako informácie, ktoré sa týkajú identifikovanej alebo

identifikovateľnej fyzickej osoby[47], teda ako informácie o osobe, ktorej totožnosť je buď preukázateľne zrejmá, alebo sa aspoň dá určiť získaním doplňujúcich informácií.

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

Osoba

Právo na ochranu údajov sa vyvinulo z práva na rešpektovanie súkromného života. Pojem súkromného života súvisí s ľudskými bytosťami. Hlavnými subjektmi, ktoré požívajú ochranu údajov, sú teda fyzické osoby. Podľa stanoviska pracovnej skupiny zriadenej podľa článku 29 je európskymi právnymi predpismi o ochrane údajov chránený len *žijúci jednotlivec*[48].

Z judikatúry ESĽP týkajúcej sa článku 8 EDĽP vyplýva, že niekedy je ťažké úplne oddeliť záležitosti súkromného a pracovného života[49].

Príklad: Vo veci *Amann/Švajčiarsko*[50] verejné orgány odpočúvali služobný telefonický hovor sťažovateľa. Na základe tohto telefonátu sťažovateľa vyšetrovali a vyplnili o ňom záznam do registra záznamov národnej bezpečnosti. Odpočúvanie sa síce týkalo služobného telefonického hovoru, ESĽP sa však domnieval, že uchovávanie údajov o tomto telefonáte súviselo so súkromným životom sťažovateľa. Súd poukázal na to, že termín „súkromný život" sa nesmie vykladať reštriktívne, a to predovšetkým preto, lebo rešpektovanie súkromného života zahŕňa právo na nadväzovanie a budovanie vzťahov s inými ľudskými bytosťami. Navyše neexistoval žiadny principiálny dôvod, ktorý by oprávňoval vylúčenie činnosti pracovnej alebo obchodnej povahy z pojmu „súkromný život". Takýto široký výklad zodpovedá výkladu podľa dohovoru č. 108. ESĽP ďalej konštatoval, že zásah v prípade sťažovateľa nebol v súlade s právnymi predpismi, keďže vnútroštátne právne predpisy neobsahujú konkrétne a podrobné ustanovenia o zhromažďovaní, zaznamenávaní a uchovávaní informácií. Súd preto dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

47 Smernica o ochrane údajov, článok 2 písm. a); dohovor č. 108, článok 2 písm. a).

48 Pracovná skupina zriadená podľa článku 29 (2007), *stanovisko 4/2007 k pojmu osobné údaje*, WP 136, 20. júna 2007, s. 22.

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

50 ESĽP, *Amann/Švajčiarsko* [VK], č. 27798/95, 16. februára 2000, bod 65.

Okrem toho, keby sa ochrana údajov mohla vzťahovať aj na otázky pracovného života, bolo by sporné, ak by sa zamerala len na fyzické osoby. Práva zakotvené v EDĽP nie sú zaručené len pre fyzické osoby, ale pre každého.

Existuje judikatúra ESĽP s rozsudkom vo veci sťažnosti právnických osôb, ktoré sa sťažovali na údajné porušenie práva na ochranu pred použitím ich údajov podľa článku 8 EDĽP. Súd však túto vec neskúmal z hľadiska súkromného života, ale z hľadiska práva na rešpektovanie obydlia a korešpondencie:

Príklad: Vec *Bernh Larsen Holding AS a iní/Nórsko*[51] sa týkala sťažnosti troch nórskych spoločností na rozhodnutie daňového úradu, ktoré im nariadilo poskytnúť daňovým kontrolórom kópiu všetkých údajov z počítačového servera využívaného všetkými tromi spoločnosťami.

ESĽP 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 EDĽP. Súd však konštatoval, že daňové orgány predložili 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 druhej strane. Súd dospel k záveru, že nedošlo k žiadnemu porušeniu článku 8.

Podľa 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. **Právne predpisy EÚ o ochrane údajov** vo všeobecnosti nepokrývajú ochranu právnických osôb, pokiaľ ide o spracovanie údajov, ktoré sa ich týkajú. Regulácia v tejto veci je na slobodnom rozhodnutí vnútroštátnych regulátorov[52].

51 ESĽP, *Bernh Larsen Holding AS a iní/Nórsko*, č. 24117/08, 14. marca 2013. Pozri taktiež ESĽP, *Liberty a iní/Spojenému kráľovstvo*, č. 58243/00, 1. júla 2008.

52 Smernica o ochrane údajov, odôvodnenie 24.

Príklad: SDEÚ vo veci *Volker a Markus Schecke a Hartmut Eifert/Land Hessen*[53] 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 [...]“[54].

Identifikovateľnosť osoby

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

- je v týchto informáciách identifikovaný jednotlivec alebo
- ak jednotlivec síce nie je v informáciách identifikovaný, ale je v nich opísaný takým spôsobom, ktorý umožňuje na základe ďalšieho skúmania zistiť, kto je dotknutou osobou.

Európskymi právnymi predpismi o ochrane údajov sa chránia oba druhy informácií rovnakým spôsobom. ESĽP opakovane konštatoval, že pojem „osobné údaje“ v EDĽP je totožný s týmto pojmom v dohovore č. 108, najmä pokiaľ ide o podmienku súvislosti s identifikovanými alebo identifikovateľnými osobami[55].

V právnych vymedzeniach osobných údajov sa ďalej nespresňuje, kedy sa osoba pokladá za identifikovanú[56]. Identifikácia si zjavne vyžaduje prvky, v ktorých sa osoba opisuje takým spôsobom, že je odlíšiteľná od všetkých ostatných osôb a rozpoznateľná ako jednotlivec. Hlavným príkladom takýchto prvkov opisu je meno osoby. Vo výnimočných prípadoch môžu mať podobný účinok ako meno ďalšie identifikačné znaky. Napríklad u verejne známych osôb postačí odkaz na postavenie danej osoby, napríklad predseda Európskej komisie.

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

54 Tamtiež, bod 52.

55 Pozri ESĽP, *Amann/Švajčiarsko* [VK], č. 27798/95, 16. februára 2000, bod 65 a ďalšie.

56 Pozri tiež ESĽP, *Odièvre/Francúzsko* [VK], č. 42326/98, 13. februára 2003 a ESĽP, *Godelli/Taliansko*, č. 33783/09, 25. septembra 2012.

Príklad: SDEÚ vo veci *Promusicae*[57] 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 [...]. Toto oznámenie informácií, ktoré sú podľa združenia Promusicae uchovávané spoločnosťou Telefónica, čo táto spoločnosť nepopiera, predstavuje spracovanie osobných údajov v zmysle článku 2 prvého odseku smernice 2002/58 v spojení s článkom 2 písm. b) smernice 95/46".

Keďže veľa mien nie je jedinečných, na určenie totožnosti osoby môžu byť potrebné dodatočné identifikačné znaky, ktoré zaistia, aby nedošlo k zámene s inou osobou. Často sa používa deň a miesto narodenia. Niektoré krajiny okrem toho zaviedli personalizované čísla s cieľom lepšie odlíšiť jednotlivých občanov. V technologickom veku sú pri identifikácii osôb čoraz dôležitejšie biometrické údaje, napríklad odtlačky prstov, digitálne fotografie alebo snímky dúhovky.

Pri uplatňovaní európskych právnych predpisov o ochrane údajov však nie nutná vysokokvalitná identifikácia dotknutej osoby. Stačí, aby príslušná osoba bola identifikovateľná. Osoba sa považuje za identifikovateľnú vtedy, ak informácie o nej obsahujú identifikačné prvky, prostredníctvom ktorých túto osobu možno priamo alebo nepriamo identifikovať[58]. Podľa odôvodnenia 26 smernice o ochrane údajov spočíva hraničné kritérium v tom, či je alebo nie je pravdepodobné, že predvídateľní používatelia informácií vrátane príjemcov tretích strán (pozri oddiel 2.3.2) budú mať k dispozícii primerané prostriedky na identifikáciu a využijú ich.

Príklad: Miestny úrad sa rozhodol, že začne zbierať údaje o rýchlosti vozidiel 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 pre takýto zber údajov žiadnu právnu oporu v právnych predpisoch o ochrane údajov. Miestny úrad namieta, že nezbiera osobné údaje. Štátne poznávacie značky sú podľa jeho názoru údaje o anonymných osobách. Miestny úrad nemá žiadne oprávnenie na prístup do

57 SDEÚ, C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 29. Januára 2008, bod 45.

58 Smernica o ochrane údajov, článok 2 písm. a).

celoštátneho registra motorových vozidiel na účely zistenia totožnosti vlastníka vozidla alebo vodiča.

Toto odôvodnenie nie je v súlade s odôvodnením 26 smernice o ochrane údajov. Keďže účelom zberu údajov je preukázateľne identifikácia a pokutovanie vodičov, ktorí prekročia predpísanú rýchlosť, predpokladá sa snaha o identifikáciu osôb. Aj keď miestne orgány nemajú prostriedky na priamu identifikáciu, postúpia údaje príslušnému orgánu, teda polícii, ktorá takéto prostriedky má. Odôvodnenie 26 takisto výslovne zahŕňa situáciu, 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 úradu rovnocenná so zberom údajov o identifikovateľných osobách, a preto si vyžaduje právny základ v právnych predpisoch o ochrane údajov.

V právnych predpisoch Rady Európy sa identifikovateľnosť chápe podobne. V článku 1 ods. 2 odporúčania o platobných údajoch[59] sa napríklad uvádza, že osoba sa nepovažuje za „identifikovateľnú", ak si identifikácia vyžaduje neprimeraný čas, náklady alebo pracovnú silu.

Autentifikácia

Ide o postup, prostredníctvom ktorého je osoba schopná dokázať, že má určitú totožnosť a/alebo je oprávnená urobiť určité veci, 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 kontrole. Ďalším prostriedkom autentifikácie je žiadosť o uvedenie informácií, ktoré by mala poznať len osoba s určitou totožnosťou alebo autentifikáciou, napríklad osobného identifikačného čísla (PIN) alebo hesla, alebo požiadanie o predloženie určitého tokenu, ktorý by mala vlastniť výlučne osoba s určitou totožnosťou alebo autentifikáciou, napríklad špeciálnej čipovej karty alebo kľúča k bankovému sejfu. Medzi mimoriadne účinné nástroje na identifikáciu a autentifikáciu osoby v rámci elektronickej komunikácie patria okrem hesiel alebo čipových kariet, niekedy spojených s kódom PIN, aj elektronické podpisy.

59 Rada Európy, Výbor ministrov (1990), odporúčanie č. R Rec(90) 19 o ochrane osobných údajov používaných pri platbách ďalších súvisiacich operáciách, 13. septembra 1990.

Povaha údajov

Ľubovoľné informácie môžu byť osobnými údajmi, ak sa týkajú osoby.

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

Osobné údaje zahŕňajú informácie týkajúce sa súkromného života osoby, ako aj informácie o jej pracovnom či verejnom živote.

ESĽP vo veci *Amann*[60] vyložil termín „osobné údaje" tak, že nie je obmedzený na záležitosti súkromnej sféry jednotlivca (pozri oddiel 2.1.1). Z toho vyplýva, že termín „osobné údaje" je relevantný taktiež pre smernicu o ochrane údajov:

Príklad: SDEÚ vo veci *Volker a Markus Schecke a Hartmut Eifert/Land Hessen*[61] konštatoval, že „v tejto súvislosti nemá nijaký význam skutočnosť, že uverejňované údaje sa týkajú profesijných činností [...]. Európsky súd pre ľudské práva v tomto ohľade v súvislosti s výkladom článku 8 EDĽP rozhodol, že pojem „súkromný život" sa nemôže vykladať reštriktívne a že „žiadny principiálny dôvod neumožňuje vylúčiť profesijné činnosti... z pojmu ‚súkromný'...".

Údaje súvisia s osobami aj vtedy, keď obsah informácií nepriamo odhaľuje údaje o osobe. V niektorých prípadoch, v ktorých existuje úzke prepojenie medzi predmetom alebo udalosťou (napr. mobilným telefónom, automobilom, nehodou) na jednej strane a osobou (napríklad majiteľom, používateľom či obeťou) na druhej strane, treba informácie o predmete alebo udalosti takisto považovať za osobné údaje.

Príklad: Vo veci *Uzun/Nemecko*[62] bol nariadený sledovanie sťažovateľa a ďalšieho muža s použitím zariadenia globálneho polohového systému (GPS)

60 Pozri ESĽP, *Amann/Švajčiarsko*, č. 27798/95, 16. februára 2000, bod 65.

61 Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen*, 9. Novembra 2010, bod 59.

62 ESĽP, *Uzun/Nemecko*, č. 35623/05, 2. septembra 2010.

namontovaného v automobile druhého uvedeného muža, a to na základe podozrenia z účasti na bombových útokoch. ESĽP v tejto veci konštatoval, že sledovanie sťažovateľa prostredníctvom systému GPS predstavovalo zásah do jeho súkromného života, ktorý je chránený na základe článku 8 EDĽP. Dohľad prostredníctvom systému GPS však bol v súlade s právnymi predpismi a bol primeraný legitímnemu cieľu vyšetrenia niekoľkých pokusov o vraždu, preto bol v demokratickej spoločnosti nutný. Súd dospel k záveru, že nedošlo k porušeniu článku 8 EDĽP.

Podoba údajov

Podoba, v akej sa osobné údaje uchovávajú alebo používajú, nie je pre uplatniteľnosť právnych predpisov o ochrane údajov relevantná. Písomné alebo ústne oznámenia môžu obsahovať osobné údaje, ako aj snímky[63] vrátane záznamu kamerového systému[64] alebo zvukového záznamu[65]. Osobnými údajmi môžu byť elektronicky zaznamenané informácie, ako aj informácie na papieri, dokonca aj vzorky buniek ľudského tkaniva, keďže zaznamenávajú DNA osoby.

2.1.2. Osobitné kategórie osobných údajov

V rámci právnych predpisov EÚ, ako aj **právnych predpisov Rady Európy**, existujú osobitné kategórie osobných údajov, ktoré môžu po spracovaní predstavovať riziko pre dotknuté subjekty z dôvodu svojej povahy, a vyžadujú rozšírenú ochranu. Spracovanie týchto osobitných kategórií údajov (tzv. citlivých údajov) smie byť povolené len so špecifickými zárukami.

Pri vymedzení pojmu citlivé údaje sú v dohovore č. 108 (článok 6) a v smernici o ochrane údajov (článok 8) vymenované nasledujúce kategórie:

- osobné údaje odhaľujúce rasový alebo etnický pôvod;
- osobné údaje odhaľujúce politické názory, náboženské alebo iné presvedčenie;

63 ESĽP, *Von Hannover/Nemecko*, č. 59320/00, 24. júna 2004; ESĽP, *Sciacca/Taliansko*, č. 50774/99, 11. januára 2005.

64 ESĽP, *Peck/Spojené kráľovstvo*, č. 44647/98, 28. januára 2003; ESĽP, *Köpke/Nemecko*, č. 420/07, 5. októbra 2010.

65 Smernica o ochrane údajov, odôvodnenia 16 a 17; ESĽP, *P.G. a J.H./Spojené kráľovstvo*, č. 44787/98, 25. septembra 2001, body 59 a 60; ESĽP, *Wisse/Francúzsko*, č. 71611/01, 20. decembra 2005.

- osobné údaje týkajúce sa zdravotného stavu alebo sexuálneho života.

> Príklad: SDEÚ v prípade *Bodil Lindqvist*[66] konštatoval, že „údaj o tom, že si určitá osoba poranila nohu a je čiastočne práceneschopná, je osobným údajom týkajúcim sa zdravia v zmysle článku 8 ods. 1 smernice 95/46".

V smernici o ochrane údajov sa k citlivým údajom dodáva „členstvo v odborových zväzoch", keďže takáto informácia môže byť dôležitým ukazovateľom politického presvedčenia alebo náklonnosti.

V dohovore č. 108 sa za osobné údaje považujú aj údaje týkajúce sa odsúdenia.

V článku 8 ods. 7 smernice o ochrane údajov sa členským štátom EÚ ukladá, aby „stanovili podmienky, za ktorých bude možné spracovávať štátne identifikačné číslo alebo akýkoľvek iný identifikačný znak všeobecného uplatnenia".

2.1.3. Anonymizované a pseudonymizované údaje

Podľa zásady obmedzeného zadržiavania údajov uvedenej v smernici o ochrane údajov, ako aj v dohovore č. 108 (ktorá je podrobnejšie vysvetlená v kapitole 3) sa údaje musia udržiavať „vo forme, ktorá umožňuje identifikáciu osôb pracujúcich s údajmi počas obdobia, ktoré je nevyhnutné na účely, pre ktoré boli údaje zhromažďované, alebo pre ktoré sú ďalej spracovávané"[67]. Ak chce teda prevádzkovateľ uchovávať údaje, ktoré už nie sú aktuálne a neslúžia na pôvodný účel, musí ich anonymizovať.

Anonymizované údaje

Údaje sú anonymizované vtedy, keď boli zo súboru údajov odstránené všetky identifikačné prvky. V informáciách nesmú byť ponechané žiadne prvky, ktoré by mohli po vynaložení primeraného úsilia slúžiť na opätovnú identifikáciu dotknutej osoby či osôb[68]. Úspešne anonymizované údaje už nie sú osobnými údajmi.

Ak osobné údaje prestanú slúžiť počiatočnému účelu, ale budú sa uchovávať v personalizovanej podobe na historické, štatistické alebo vedecké účely, v smernici

66 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003, bod 51.

67 Smernica o ochrane údajov, článok 6 ods. 1 písm. e) a dohovor č. 108, článok 5 písm. e).

68 Tamtiež, odôvodnenie 26.

o ochrane údajov a dohovore č. 108 sa takýto postup umožňuje pod podmienkou uplatnenia primeraného zabezpečenia pred zneužitím[69].

Pseudonymizované údaje

Osobné informácie obsahujú identifikačné znaky, napríklad meno, dátum narodenia, pohlavie a adresu. Ak sú osobné informácie pseudonymizované, identifikačné znaky sa nahradia jedným pseudonymom. Pseudonymizácia sa dosiahne napríklad zašifrovaním identifikačných znakov v osobných údajoch.

V právnych vymedzeniach pojmov v dohovore č. 108 ani v smernici o ochrane údajov sa pseudonymizované údaje výslovne neuvádzajú. V článku 42 vysvetľujúcej správy k dohovoru č. 108 sa však uvádza, že „požiadavka [...] na časový limit uchovávania údajov vo forme súvisiacej s menom neznamená, že údaje by sa mali po určitom čase nezvratne oddeliť od mena osoby, ktorej sa týkajú, znamená to len toľko, že by nemalo byť bez problémov možné spojiť údaje a identifikačné znaky". Tento výsledok je možné dosiahnuť pseudonymizáciou údajov. Bez šifrovacieho kľúča pseudonymizované údaje je možné identifikovať len s ťažkosťou. Prepojenie s totožnosťou však naďalej existuje vo forme pseudonymu plus šifrovacieho kľúča. Pre tých, ktorí majú oprávnenie použiť šifrovací kľúč, je opätovná identifikácia ľahko uskutočniteľná. Treba sa osobitne chrániť pred použitím šifrovacích kľúčov neoprávnenými osobami.

Keďže pseudonymizácia údajov je jedným z najdôležitejších prostriedkov zaistenia rozsiahlej ochrany údajov v prípadoch, keď úplne ukončenie používania osobných údajov nie je možné, treba podrobnejšie vysvetliť logiku a účinok tohto opatrenia.

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".

69 Smernica o ochrane údajov, článok 6 ods. 1 písm. e) a dohovor č. 108, článok 5 písm. e).

Používatelia, ktorí budú mať prístup k týmto údajom, zvyčajne nebudú schopní identifikovať „324“ alebo „YESz3201“ ako „Karol Novák, narodený 3. apríla 1967“. Je teda pravdepodobnejšie, že pseudonymizované údaje nebudú zneužité.

Prvý príklad je 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 nebude zložité. Spôsob pseudonymizácie ovplyvňuje účinnosť ochrany údajov.

Osobné údaje so zašifrovanými identifikačnými znakmi sa používajú v mnohých situáciách ako prostriedky na utajenie 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 subjektov. Ide napríklad o prípady, keď výskumník skúma priebeh choroby u 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 zlepšenie ochrany súkromia. Môže fungovať ako významná súčasť ochrany súkromia už v štádiu návrhu. Znamená to, že ochrana údajov sa stane súčasťou štruktúry pokročilých systémov spracovania údajov.

2.2. Spracúvanie údajov

Hlavné body

- Termín „spracúvanie“ odkazuje predovšetkým na automatizované spracúvanie.
- V rámci právnych predpisov EÚ, sa „spracúvanie“ ďalej týka manuálneho spracúvania v štruktúrovaných archivačných systémoch.
- V rámci právnych predpisov Rady Európy, význam pojmu „spracúvanie“ možno rozšíriť o vnútroštátne právne predpisy s cieľom zahrnúť manuálne spracovanie.

Ochrana údajov podľa dohovoru č. 108 a smernice o ochrane údajov sa zameriava predovšetkým na automatizované spracúvanie údajov.

V **právnych predpisoch Rady Európy** sa v definícii automatického spracúvania uznáva, že medzi automatizovanými operáciami môžu byť potrebné niektoré fázy ručného používania osobných údajov. Podobne **v právnych predpisoch EÚ** je

automatizované spracúvanie údajov vymedzené ako „operácie, ak sa úplne alebo čiastočne vykonávajú automatickými prostriedkami“[70].

Príklad: SDEÚ vo veci *Bodil Lindqvist*[71] konštatoval:

„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 95/46“.

Manuálne spracúvanie údajov si takisto vyžaduje ochranu údajov.

Ochrana údajov **podľa právnych predpisov EÚ** rozhodne nie je obmedzená na automatizované spracúvanie údajov. Podľa právnych predpisov EÚ sa ochrana údajov uplatňuje na spracúvanie osobných údajov v manuálnom archivačnom systéme, teda v špeciálne štruktúrovanom súbore vytlačenom na papieri[72]. Dôvod takéhoto rozšírenia ochrany údajov je:

- súbory vytlačené na papieri je možné usporiadať takým spôsobom, ktorým sa zrýchli a zjednoduší hľadanie informácií;

- uchovávanie osobných údajov v štruktúrovaných súboroch vytlačených na papieri uľahčuje obchádzanie obmedzení stanovených právnymi predpismi pre automatizované spracúvanie údajov[73].

V rámci právnych predpisov Rady Európy sa dohovorom č. 108 sa reguluje predovšetkým spracúvanie údajov v automatizovaných súboroch údajov[74]. Takisto sa stanovuje možnosť rozšíriť ochranu vo vnútroštátnych právnych predpisoch na manuálne spracúvanie. Mnohé zmluvné strany dohovoru č. 108 využili túto možnosť a predložili v tomto zmysle vyhlásenia generálnemu tajomníkovi Rady Európy[75].

70 Dohovor č. 108, článok 2 písm. c); smernica o ochrane údajov, článok 2 písm. b) a článok 3 ods. 1.

71 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003, bod 27.

72 Smernica o ochrane údajov, článok 3 ods. 1.

73 Tamtiež, odôvodnenie 27.

74 Dohovor č. 108, článok 2 písm. b).

75 Pozri vyhlásenia pripravené na základe dohovoru č. 108, článok 3 ods. 2 písm. c).

Rozšírenie ochrany údajov podľa takéhoto vyhlásenia sa musí týkať celého manuálneho spracúvania údajov a nemôže sa obmedziť len na spracúvanie v manuálnych archivačných systémoch[76].

Pokiaľ ide o povahu zahrnutých operácií spracúvania, pojem „spracúvanie" je súhrnný v rámci **právnych predpisov EÚ aj právnych predpisov Rady Európy**: „spracúvanie osobných údajov" [...] znamená akúkoľvek operáciu [...], ako je zber, zaznamenávanie, organizácia, uskladnenie, úprava alebo nahradenie, vyhľadávanie, nahliadnutie, používanie, odhalenie prenosom, šírenie alebo sprístupnenie iným spôsobom, upravenie alebo kombinácia, blokovanie, vymazanie alebo zničenie"[77] vykonané na osobných údajoch. Termín „spracúvanie" takisto zahŕňa kroky, v rámci ktorých prestáva byť za údaje zodpovedný jeden prevádzkovateľ a zodpovednosť sa presúva na druhého prevádzkovateľa.

Príklad: Zamestnávatelia zbierajú a spracúvajú údaje o svojich zamestnancoch vrátane informácií týkajúcich sa miezd. Právnym základom legitímnosti tejto činnosti je pracovná zmluva.

Zamestnávatelia musia predkladať údaje o svojich zamestnancoch daňovým úradom. Predkladanie údajov je takisto „spracúvaním" v zmysle tohto pojmu v dohovore č. 108 a v smernici. Právnym základom takéhoto uverejnenia nie je pracovná zmluva. Musí existovať dodatočný právny základ pre operácie spracúvania, ktorý oprávňuje prenos údajov o mzdách od zamestnávateľa daňovému úradu. Tento právny základ je zvyčajne zahrnutý do ustanovení vnútroštátnych daňových predpisov. Bez takýchto ustanovení by bol prenos dát nezákonným spracúvaním.

2.3. Používatelia osobných údajov

Hlavné body

- Každý, kto sa rozhodne spracovať osobné údaje iných osôb, je podľa právnych predpisov o ochrane údajov „prevádzkovateľom". Ak takéto rozhodnutie prijme spoločne niekoľko osôb, môžu sa stať „spoločnými prevádzkovateľmi".

76 Pozri znenie dohovoru č. 108, článok 3 ods. 2.

77 Smernica o ochrane údajov, článok 2 písm. b). Podobne pozri aj dohovor č. 108, článok 2 písm. c).

- „Sprostredkovateľ" je právne samostatný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.
- Sprostredkovateľ sa stáva prevádzkovateľom vtedy, ak nedodrží pokyny prevádzkovateľa a použije údaje na svoj vlastný účel.
- Každý, kto prijíma údaje od prevádzkovateľa, je „príjemca".
- „Tretia strana" je fyzická alebo právnická osoba, ktorá nekoná podľa pokynov prevádzkovateľa (a nie je dotknutou osobou).
- „Príjemca tretej strany" je osoba alebo subjekt, ktorý je právne oddelený od prevádzkovateľa, ale prijíma od neho osobné údaje.

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. Prevádzkovateľom alebo sprostredkovateľom sa teda môže stať len subjekt, ktorý je podľa platných právnych predpisov schopný niesť zodpovednosť. V súkromnom sektore zvyčajne ide o fyzickú alebo právnickú osobu, vo verejnom sektore je to spravidla orgán. Iné subjekty, napríklad orgány alebo inštitúcie bez právnej subjektivity, sa môžu stať prevádzkovateľmi alebo sprostredkovateľmi len vtedy, ak sa to stanovuje v osobitných právnych ustanoveniach.

Príklad: Keď marketingové oddelenie spoločnosti Sunshine naplánuje, že bude spracúvať údaje na účely prieskumu trhu, prevádzkovateľom tohto spracovania nebude marketingové oddelenie, ale spoločnosť Sunshine. Marketingové oddelenie nemôže byť prevádzkovateľom, pretože nemá žiadnu samostatnú právnu subjektivitu.

V skupinách spoločností sa za samostatných prevádzkovateľov alebo sprostredkovateľov pokladajú materské spoločnosti a jednotlivé pobočky, ktoré sú samostatnými právnickými osobami. Dôsledkom samostatného právneho postavenia je, že prenos údajov medzi členmi skupiny spoločností si bude vyžadovať osobitný právny základ. Neexistuje žiadna výsada, ktorou by sa povoľovala výmenu osobných údajov ako taká medzi samostatnými právnickými osobami v rámci skupiny spoločností.

V tejto súvislosti sa treba zmieniť o úlohe súkromných osôb. **V rámci právnych predpisov EÚ** nepatria súkromné osoby, ktoré spracúvajú údaje o iných osobách v rámci

výlučne osobnej alebo domácej činnosti, do rozsahu pôsobnosti smernice o ochrane údajov a nepokladajú sa za prevádzkovateľov[78].

Jurisdikcia však stanovila, že právne predpisy o ochrane údajov sa budú uplatňovať vtedy, keď súkromná osoba pri používaní internetu uverejňuje údaje o iných osobách.

Príklad: SDEÚ vo veci *Bodil Lindqvist*[79] 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 spracovanie osobných údajov" v zmysle článku 3 ods. 1 smernice 95/46"[80].

Takéto spracovanie osobných údajov nepredstavuje výlučne osobnú alebo domácu činnosť, ktorá je mimo rozsahu pôsobnosti smernice o ochrane 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 spracúvania osobných údajov, ktoré spočíva v ich zverejnení na internete takým spôsobom, že sa sprístupnia neobmedzenému počtu osôb"[81].

Prevádzkovateľ

V právnych predpisoch EÚ sa prevádzkovateľ vymedzuje ako niekto, kto „sám, alebo v spojení s inými, určí účely a prostriedky spracovania osobných údajov"[82]. Rozhodnutím prevádzkovateľa sa stanovuje, prečo a ako sa údaje budú spracovávať. **V právnych predpisoch Rady Európy** sa vo vymedzení pojmu „prevádzkovateľ" dopĺňa, že prevádzkovateľ rozhoduje o tom, ktoré kategórie osobných údajov by sa mali uchovávať[83].

78 Smernica o ochrane údajov, odôvodnenie 12 a článok 3 ods. 2 posledná zarážka.

79 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003.

80 Tamtiež, odsek 27.

81 Tamtiež, bod 47.

82 Smernica o ochrane údajov, článok 2 písm. d).

83 Dohovor č. 108, článok 2 písm. d).

Vo vymedzení pojmu prevádzkovateľ v dohovore č. 108 sa odkazuje na ďalší aspekt kontroly, o ktorom sa treba zmieniť. Vo vymedzení sa upozorňuje na otázku, kto môže zákonne spracúvať určité údaje na určitý účel. Ak existuje podozrenie na nezákonné spracovanie údajov a musí sa zistiť, kto je zodpovedným prevádzkovateľom, bude sa za prevádzkovateľa považovať osoba alebo subjekt, napríklad spoločnosť alebo orgán, ktorý rozhodol o spracovaní údajov, a to bez ohľadu na to, či bol alebo nebol oprávnený prijať takéto rozhodnutie[84]. Žiadosť o odstránenie údajov teda vždy musí byť adresovaná „skutočnému" prevádzkovateľovi.

Spoločná kontrola

Vo vymedzení pojmu „prevádzkovateľ" v smernici o ochrane údajov sa stanovuje, že môže existovať niekoľko právne samostatných osôb, ktoré konajú ako prevádzkovatelia spoločne alebo v spojení s inými. To znamená, že spoločne rozhodujú o spracovaní údajov na spoločné účely[85]. To je však právne možné len v prípadoch, keď existuje osobitný právny základ umožňujúci spoločné spracúvanie údajov na spoločný účel.

Príklad: Bežným príkladom spoločnej kontroly je databáza o dlžníkoch 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 predpisoch sa výslovne nestanovuje, či sa pri spoločnej kontrole vyžaduje, aby všetci prevádzkovatelia mali rovnaký spoločný účel, alebo či stačí, ak sa ich účely len čiastočne prekrývajú. Zatiaľ však nie je k dispozícii žiadna relevantná jurisdikcia na európskej úrovni a nie je jasné, aké sú dôsledky, pokiaľ ide o zodpovednosť. Pracovná skupina zriadená podľa článku 29 obhajuje široký výklad pojmu spoločnej kontroly s cieľom umožniť určitú flexibilitu a reagovať na stále zložitejšiu realitu v oblasti spracovania údajov[86]. Stanovisko pracovnej skupiny dokladá prípad Spoločnosti pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT).

84 Pozri tiež: pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 1/2010 k pojmom „prevádzkovateľ" a „sprostredkovateľ"*, WP 169, Brusel, 16. februára 2010, s. 15.

85 Smernica o ochrane údajov, článok 2 písm. d).

86 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 1/2010 k pojmom „prevádzkovateľ" a „sprostredkovateľ"*, WP 169, Brusel, 16. februára 2010, s. 19.

Príklad: V tzv. veci 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 výslovného príkazu európskych bankových inštitúcií, 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 pred európskymi zákazníkmi za oznámenie ich údajov americkým orgánom[87]. Spoločnosť SWIFT sa rozhodla zverejniť údaje, čím (nezákonne) prevzala úlohu prevádzkovateľa. Bankové inštitúcie preukázateľne zanedbali povinnosť dohliadať na svojho sprostredkovateľa, a preto nemôžu byť úplne oslobodené od povinností prevádzkovateľov. Výsledkom situácie je spoločná kontrola.

Sprostredkovateľ

Sprostredkovateľ je **v rámci právnych predpisov EÚ** vymedzený ako niekto, kto spracúva osobné údaje v mene prevádzkovateľa[88]. Činnosti, ktorými je sprostredkovateľ poverený, môžu byť obmedzené na veľmi špecifickú úlohu alebo kontext alebo môžu byť pomerne všeobecné a komplexné.

Podľa právnych predpisov Rady Európy je význam pojmu sprostredkovateľ rovnaký ako podľa právnych predpisov EÚ.

Sprostredkovatelia sú okrem spracúvania údajov pre iných aj prevádzkovateľmi sami osebe, pokiaľ ide o spracúvanie údajov, ktoré vykonávajú na svoje vlastné účely, napríklad administratíva týkajúca sa ich vlastných zamestnancov, miezd a účtov.

Príklady: Spoločnosť Everready sa špecializuje na spracúvanie údajov pri spravovaní údajov o ľudských zdrojoch pre iné spoločnosti. V tejto funkcii je spoločnosť Everready sprostredkovateľom.

87 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.

88 Smernica o ochrane údajov, článok 2 písm. e).

Keď však spoločnosť Everready spracúva údaje o svojich vlastných zamestnancoch, je prevádzkovateľom operácií spracúvania údajov na účely plnenia svojich povinností ako zamestnávateľa.

Vzťah medzi prevádzkovateľom a sprostredkovateľom

Ako sme videli, prevádzkovateľ je vymedzený ako subjekt, ktorý určuje účely a prostriedky spracúvania.

Príklad: Riaditeľ spoločnosti Sunshine sa rozhodne, že spoločnosť Moonlight s odborným zameraním na analýzu trhu by mala vypracovať trhovú analýzu údajov o zákazníkoch spoločnosti Sunshine. Určením prostriedkov spracovania síce bude poverená spoločnosť Moonlight, spoločnosť Sunshine však naďalej zostáva prevádzkovateľom a spoločnosť Moonlight je len sprostredkovateľom, keďže (podľa zmluvy) spoločnosť Moonlight môže použiť údaje o zákazníkoch spoločnosti Sunshine len na také účely, ktoré určí spoločnosť Sunshine.

Aj keď je právomoc určiť prostriedky spracúvania prenesená na sprostredkovateľa, prevádzkovateľ musí byť schopný zasahovať do rozhodnutí sprostredkovateľa týkajúcich sa prostriedkov spracovania. Celkovú zodpovednosť naďalej nesie prevádzkovateľ, ktorý musí dohliadať na sprostredkovateľov, aby zaistil, že ich rozhodnutia budú v súlade s právnymi predpismi o ochrane údajov. Zmluva, v ktorej by sa prevádzkovateľovi zakazovalo zasahovať do rozhodnutí sprostredkovateľa, by sa pravdepodobne vykladala tak, že povedie k spoločnej kontrole, pri ktorej majú obe strany právnu zodpovednosť prevádzkovateľa.

Okrem toho, keby sprostredkovateľ nerešpektoval obmedzenia týkajúce sa používania údajov predpísané prevádzkovateľom, stal by sa prevádzkovateľom aspoň do tej miery, do akej porušil pokyny prevádzkovateľa. Sprostredkovateľ by sa s najväčšou pravdepodobnosťou stal prevádzkovateľom, ktorý koná nezákonne. Na druhej strane by pôvodný prevádzkovateľ musel vysvetliť, ako sprostredkovateľ mohol prekročiť svoj mandát. Pracovná skupina zriadená podľa článku 29 sa prikláňa k tomu, že v takýchto prípadoch predpokladá spoločnú kontrolu, keďže vedie k najlepšej ochrane záujmov dotknutých osôb[89]. Dôležitým dôsledkom spoločnej kontroly

89 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 1/2010 k pojmom „prevádzkovateľ" a „spracovateľ"*, WP 169, Brusel, 16. februára 2010, s. 25 a 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.

by mala byť spoločná a nerozdielna zodpovednosť za škody, ktorá ponúka dotknutým osobám viac nápravných prostriedkov.

Problémy s rozdelením zodpovednosti môžu nastať aj v prípade, že prevádzkovateľom je malý podnik a sprostredkovateľom veľká obchodná spoločnosť s právnou subjektivitou, ktorá má moc diktovať podmienky poskytovania svojich služieb. Za takýchto okolností pracovná skupina zriadená podľa článku 29 potvrdzuje, že štandard zodpovednosti by sa nemal znižovať na základe hospodárskej nerovnováhy a že je nutné zachovať výklad pojmu prevádzkovateľ[90].

V záujme jasnosti a transparentnosti by sa podrobnosti o vzťahu medzi prevádzkovateľom a sprostredkovateľom mali zaznamenať v písomnej zmluve[91]. Ak takáto zmluva nebola uzatvorená, ide o porušenie povinnosti prevádzkovateľa poskytnúť písomné doklady o vzájomnej zodpovednosti, ktoré môže viesť k postihom[92].

Sprostredkovateľ môže poveriť určitými úlohami ďalších čiastočných sprostredkovateľov. Je to právne prípustné a konkrétne závisí od zmluvných dojednaní medzi prevádzkovateľom a sprostredkovateľom vrátane ustanovenia o tom, či je potrebné povolenie prevádzkovateľa pri každom jednotlivom prípade alebo či stačí len informovanie.

V rámci právnych predpisov Rady Európy v celom rozsahu sa uplatňuje výklad pojmov prevádzkovateľ a sprostredkovateľ, ako je uvedený v predchádzajúcom texte, ako dokazujú odporúčania vypracované podľa dohovoru č. 108[93].

2.3.2. Príjemcovia 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 prístupu k osobným údajom uchovávaným prevádzkovateľom.

90 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 1/2010 k pojmom „prevádzkovateľ" a sprostredkovateľ"*, WP 169, Brusel, 16. februára 2010, s. 26.

91 Smernica o ochrane údajov, článok 17 ods. 3 a 4.

92 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 1/2010 k pojmom „prevádzkovateľ" a sprostredkovateľ"*, WP 169, Brusel, 16. februára 2010, s. 27.

93 Pozri napríklad odporúčanie o profilovaní, článok 1.

„Tretia strana“ je subjekt, ktorý sa právne odlišuje od prevádzkovateľa. Zverejnenie údajov tretím stranám si preto bude vždy vyžadovať špecifický právny základ. Podľa článku 2 písm. f) smernice o ochrane údajov tretia strana znamená „akúkoľvek fyzickú alebo právnickú osobu, štátny orgán, agentúru alebo akýkoľvek iný orgán, ako údajový subjekt, ten, kto spracovanie riadi, spracovateľ a osoby, ktoré sú na základe priameho poverenia kontrolóra alebo spracovateľom poverené spracovať údaje“. To znamená, že osoby pracujúce pre organizáciu, ktorá je právne odlišná od prevádzkovateľa, dokonca aj keď patrí do rovnakej skupiny alebo holdingovej spoločnosti, budú „treťou stranou“ (alebo patria k tretej strane). Na druhej strane „tretími stranami“ by nemali byť pobočky bánk, ktoré spracúvajú účty zákazníkov pod priamym dozorom svojho vedenia[94].

„Príjemca“ je širší termín než „tretia strana“. V zmysle článku 2 písm. g) smernice o ochrane údajov príjemca znamená „fyzickú alebo právnickú osobu, štátny orgán, agentúru alebo akýkoľvek iný orgán, pre ktorý sa údaje odhaľujú, či to je tretia strana alebo nie“. Príjemcom 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 rovnakej spoločnosti alebo orgánu.

Rozdiel medzi príjemcami a tretími stranami je dôležitý nielen z hľadiska podmienok zákonného zverejnenia údajov. Zamestnanci prevádzkovateľa alebo sprostredkovateľa môžu byť bez ďalších právnych požiadaviek príjemcami osobných údajov, ak sa podieľajú na operáciách spracovania prevádzkovateľa alebo sprostredkovateľa. Na druhej strane tretia strana, ktorá je právne nezávislá od prevádzkovateľa alebo sprostredkovateľa, nie je oprávnená používať osobné údaje spracúvané prevádzkovateľom, okrem osobitných prípadov so špecifickými právnymi dôvodmi. „Príjemcovia tretích strán“, ktorí prijímajú údaje, preto budú vždy potrebovať právny základ pre zákonné prijímanie osobných údajov.

Príklad: Zamestnanec sprostredkovateľa, ktorý používa osobné údaje pri plnení úloh, ktorými ho zamestnávateľ poveril, je príjemcom údajov, nie je však treťou stranou, keďže používa údaje v mene sprostredkovateľa a podľa jeho pokynov.

Ak sa však tento zamestnanec rozhodne použiť údaje, ku ktorým má prístup ako zamestnanec sprostredkovateľa, na svoje vlastné účely a predá ich inej

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

spoločnosti, koná ako tretia strana. Nedodržiava už pokyny sprostredkovateľa (zamestnávateľa). Zamestnanec by ako tretia strana potreboval právny základ na nadobudnutie a predaj údajov. V tomto príklade zamestnanec určite takýto právny základ nemá, takže jeho kroky sú nezákonné.

2.4. Súhlas

Hlavné body

- Súhlas ako právny základ pre spracovanie osobných údajov musí byť slobodný, informovaný a špecifický.
- Súhlas musí byť poskytnutý jednoznačne. Súhlas musí byť poskytnutý výslovne alebo musí vyplývať z takého spôsobu konania, ktorý nevyvoláva žiadne pochybnosti o tom, že dotknutá osoba súhlasí so spracovaním svojich údajov.
- Spracovanie citlivých údajov na základe súhlasu si vyžaduje výslovný súhlas.
- Súhlas je možné kedykoľvek zrušiť.

Súhlas znamená „slobodne poskytnutú a informovanú indikáciu prianí" dotknutej osoby[95]. V mnohých prípadoch predstavuje právny základ pre legitímne spracovanie údajov (pozri oddiel 4.1).

2.4.1. Prvky platného súhlasu

V právnych predpisoch EÚ sa stanovujú tri prvky, ktoré sú podmienkou platnosti súhlasu a ktoré zaručujú, že dotknuté osoby skutočne mali v úmysle súhlasiť s použitím svojich údajov:

- dotknuté osoby nesmú byť pri vyjadrení súhlasu vystavené žiadnemu tlaku;
- dotknuté osoby musia byť náležite informované o cieli a dôsledkoch vyslovenia súhlasu;
- rozsah súhlasu musí byť primerane konkrétny.

95 Smernica o ochrane údajov, článok 2 písm. h).

Súhlas bude platný v zmysle právnych predpisov o ochrane údajov len vtedy, ak sú splnené všetky uvedené požiadavky.

Dohovor č. 108 neobsahuje vymedzenie súhlasu a ponecháva ho na domáce právne predpisy. Prvky platného súhlasu **v právnych predpisoch Rady Európy** zodpovedajú opísaným prvkom, ako sú stanovené v odporúčaniach, ktoré boli vypracované na základe dohovoru č. 108[96]. Požiadavky na súhlas sú rovnaké ako pri platnom vyhlásení o úmysle podľa občianskoprávnych predpisov EÚ.

Dodatočné občianskoprávne požiadavky na platnosť súhlasu, napríklad právna spôsobilosť, prirodzene platia aj v kontexte ochrany údajov, keďže takéto požiadavky predstavujú základné predpokladané právne podmienky. Dôsledkom neplatného súhlasu osôb, ktoré nie sú právne spôsobilé, bude neexistencia právneho základu pre spracovanie údajov o takýchto osobách.

Súhlas možno vyjadriť buď výslovne[97], alebo nevýslovne. Výslovný súhlas nevyvoláva žiadne pochybnosti o úmysloch dotknutej osoby a môže byť vyjadrený buď ústne alebo písomne. Nevýslovný súhlas sa odvodzuje od okolností. Každý súhlas musí byť vyjadrený jednoznačne[98]. To znamená, že by nemali existovať žiadne odôvodnené pochybnosti o tom, že dotknutá osoba chcela vyjadriť súhlas so spracovaním svojich údajov. Napríklad jednoznačný súhlas nemôže byť odvodený výlučne z nečinnosti dotknutej osoby. Ak sú údaje určené na spracovanie citlivé, výslovný súhlas je záväzný a musí byť jednoznačný.

Slobodný súhlas

Existencia slobodného súhlasu je platná iba vtedy, „ak si dotknutá osoba skutočne môže vybrať a neexistuje riziko podvodu, zastrašovania, nátlaku alebo významných negatívnych následkov, ak dotknutá osoba nebude súhlasiť“[99].

Príklad: Na viacerých letiskách musia cestujúci prechádzať cez telesné skenery, aby sa dostali do oblasti na nastupovanie[100]. Vzhľadom na to, že počas

96 Pozri napríklad dohovor č. 108, odporúčanie o štatistických údajoch, bod 6.

97 Smernica o ochrane údajov, článok 8 ods. 2.

98 Tamtiež, článok 7 písm. a) a článok 26 ods. 1.

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

100 Príklad je prevzatý odtamtiež, s. 15.

skenovania sa spracúvajú údaje cestujúcich, spracovanie musí byť v súlade s jedným z právnych základov podľa článku 7 smernice o ochrane údajov (pozri oddiel 4.1.1). Prechod cez telesné skenery sa niekedy prezentuje ako možnosť pre cestujúcich, z čoho vyplýva, že spracovanie by mohlo byť zdôvodnené už na základe ich súhlasu. Cestujúci sa však môžu obávať, že ak odmietnu prejsť cez telesný skener, vzbudia podozrenie alebo budú nútení podrobiť sa dodatočným kontrolám, napríklad telesnej prehliadke. Mnohí cestujúci poskytnú svoj súhlas so skenovaním, pretože sa tak vyhnú potenciálnym problémom alebo meškaniu. Takýto súhlas nie je dostatočne slobodný.

Pevný legitímny základ je preto možné nájsť len v akte zákonodarcu, a to v článku 7 písm. e) smernice o ochrane údajov, z ktorého vyplýva povinnosť cestujúcich spolupracovať, keďže ide o nadradený verejný záujem. V tomto právnom predpise by sa mohla stanoviť možnosť výberu medzi skenovaním a osobnou prehliadkou, ale len ako súčasť dodatočných opatrení pohraničnej kontroly nutných za určitých okolností. Takto to stanovila Európska komisia v dvoch nariadeniach týkajúcich sa bezpečnostných skenerov z roku 2011[101].

Sloboda pri poskytnutí súhlasu byť mohla byť ohrozená v podriadenom postavení, keď existuje významný hospodársky alebo iný rozdiel medzi prevádzkovateľom zabezpečujúcim súhlas a dotknutou osobou, ktorá súhlas poskytuje[102].

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 navrhuje pridať do adresára fotografie jednotlivých zamestnancov, aby sa napríklad uľahčilo rozpoznávanie kolegov na stretnutiach. Zástupcovia zamestnancov požadujú, aby pridanie fotografie bolo podmienené súhlasom jednotlivých zamestnancov.

101 Nariadenie Komisie (EÚ) č. 1141/2011 z 10. Novembra 2011, ktorým sa mení a dopĺňa nariadenie (ES) č. 272/2009, ktorým sa dopĺňajú spoločné základné normy bezpečnostnej ochrany civilného letectva, pokiaľ ide o používanie bezpečnostných skenerov na letiskách EÚ, Ú. v. EÚ L 293, 2011 a vykonávacie nariadenie Komisie (EÚ) č. 1147/2011 z 11. Novembra 2011, ktorým sa mení a dopĺňa nariadenie (EÚ) č. 185/2010 o vykonávaní spoločných základných noriem bezpečnostnej ochrany civilného letectva, pokiaľ ide o používanie bezpečnostných skenerov na letiskách EÚ, Ú. v. EÚ L 294, 2011.

102 Pozri tiež: pracovná skupina zriadená podľa článku 29 (2001), *stanovisko 8/2001 o spracovaní osobných údajov v súvislosti so zamestnaním*, WP 48, Brusel, 13. septembra 2001 a 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.

V takom prípade by sa súhlas zamestnanca mal pokladať za právny základ spracovania fotografií v adresári, keďže je jasné, že uverejnenie fotografie v adresári ako také nemá negatívny vplyv, navyše je veľmi pravdepodobné, že ak zamestnanec odmietne uverejnenie svojej fotografie v adresári, nebude to preňho mať žiadne negatívne dôsledky zo strany zamestnávateľa.

To však neznamená, že súhlas nikdy nemôže byť platný za okolností, keď by jeho odmietnutie malo negatívne dôsledky. Napríklad, keď nesúhlas s vlastníctvom zákazníckej karty v supermarkete vedie len k tomu, že zákazník nemá nárok na zníženie ceny určitého tovaru, súhlas zostáva platným právnym základom pre spracúvanie osobných údajov tých zákazníkov, ktorí súhlasili s vystavením takejto karty. Medzi zákazníkom a supermarketom nie je vzťah podriadenosti a dôsledky neposkytnutia súhlasu nie sú natoľko závažné, aby dotknutej osobe bránili v slobodnom výbere.

Ak však dostatočne dôležitý tovar alebo služby možno získať len a výlučne pod podmienkou poskytnutia určitých osobných údajov tretím stranám, súhlas dotknutej osoby so zverejnením jej údajov zvyčajne nie je možné pokladať za slobodný výber, a preto podľa právnych predpisov o ochrane údajov nie je platný.

Príklad: Súhlas cestujúcich s tým, aby letecká spoločnosť preniesla tzv. osobné záznamy o cestujúcom (PNR), konkrétne údaje o jeho totožnosti, stravovacích návykoch alebo zdravotných problémoch, imigračným orgánom určitého cudzieho štátu nemožno pokladať za platný súhlas podľa právnych predpisov o ochrane údajov, keďže cestujúci nemajú iný výber, ak chcú navštíviť danú krajinu. Ak má byť prenos takýchto údajov zákonný, je potrebné prijať iný právny základ než súhlas: s najväčšou pravdepodobnosťou osobitný právny predpis.

Informovaný súhlas

Dotknutá osoba musí mať pred prijatím rozhodnutia dostatok informácií. Dostatočnosť poskytnutých informácií je možné posúdiť len individuálne v jednotlivých prípadoch. Informovaný súhlas zvyčajne zahŕňa presný a zrozumiteľný opis veci, ktorá si vyžaduje súhlas, a ďalej prehľad dôsledkov poskytnutia alebo odmietnutia súhlasu. Jazykové prostriedky poskytnutých informácií by mali byť prispôsobené predpokladaným adresátom.

Informácie musia byť ľahko pre dotknutú osobu ľahko dostupné. Prístupnosť a viditeľnosť informácií predstavujú dôležité prvky. V prostredí on-line môžu byť dobrým riešením viacúrovňové oznámenia, keďže dotknutá osoba získa prístup nielen k stručnej, ale aj k rozsiahlejšej verzii informácií.

Špecifikovaný súhlas

Aby bol súhlas platný, musí byť špecifikovaný. Špecifikovaný súhlas úzko súvisí s kvalitou informácií o predmete súhlasu. V tejto súvislosti budú relevantné primerané očakávania priemernej dotknutej osoby. Ak sa majú pridať alebo zmeniť postupy spracovania takým spôsobom, ktorý nebolo možné primerane predpokladať pri poskytnutí prvého súhlasu, je potrebné požiadať dotknutú osobu o opätovný súhlas.

Príklad: SDEÚ sa vo veci *Deutsche Telekom AG*[103] zaoberal otázkou, či poskytovateľ telekomunikačných služieb, ktorý musel postúpiť osobné údaje predplatiteľov na základe článku 12 *smernice o súkromí a elektronických komunikáciách*[104], potreboval obnovený súhlas od dotknutých osôb, keďže pri poskytnutí pôvodného súhlasu neboli uvedení príjemcovia.

SDEÚ dospel k záveru, že podľa uvedeného článku nebolo nutné obnovovať súhlas pred postúpením údajov, keďže dotknuté osoby mali podľa uvedeného ustanovenia možnosť vysloviť súhlas len na účel spracovania, ktorým bolo uverejnenie ich údajov, a nemohli si vybrať rôzne telefónne zoznamy, v ktorých by tieto údaje mohli byť uverejnené.

Súdny dvor 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“[105]. Okrem toho účastníka nepoškodí to, kto je autorom zverejnenia,

103 SDEÚ, C-543/09, *Deutsche Telekom AG/Nemecko*, 5. mája 2011, pozri najmä body 53 a 54.

104 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.

105 SDEÚ, C-543/09, *Deutsche Telekom AG/Nemecko*, 5. Mája 2011, pozri najmä bod 61.

ale „samotné zverejnenie osobných údajov v telefónnom zozname, ktorý má osobitný účel, môže účastníka poškodiť“[106].

2.4.2. Právo zrušenia súhlasu v ľubovoľnom čase

V smernici o ochrane údajov sa neuvádza všeobecné právo zrušenia súhlasu v ľubovoľnom čase. V podstate sa však predpokladá, že takéto právo existuje a že dotknutá osoba musí mať možnosť uplatniť toto právo podľa vlastného uváženia. Nemalo by sa požadovať vysvetlenie dôvodov zrušenia a nemalo by hroziť žiadne riziko negatívnych následkov okrem ukončenia prípadných výhod, ktoré vyplývali z odsúhlaseného používania údajov.

Príklad: Zákazník súhlasí so zasielaním reklamných e-mailov na adresu, ktorú poskytol prevádzkovateľovi. Ak zákazník svoj súhlas zruší, prevádzkovateľ musí ihneď zastaviť zasielanie reklamných e-mailov. Nesmie zákazníkovi ukladať žiadne postihy, napríklad poplatky.

Ak zákazník súhlasil s použitím svojich údajov na účely zasielania reklamných e-mailov a za odmenu mal nárok na 5 % zníženie ceny za ubytovanie v hoteli, neskoršie zrušenie súhlasu so zasielaním reklamných e-mailov by nemalo viesť k tomu, že zákazník bude musieť vrátiť poskytnutú zľavu.

106 Tamtiež, pozri najmä bod 62.

3

Hlavné zásady európskeho práva v oblasti ochrany údajov

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov, článok 6 ods. 1 písm. a) a b) SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland* 16. decembra 2008 SDEÚ, Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert /Land Hessen*, 9. novembra 2010	**Zásada zákonného spracúvania**	Dohovor č. 108, článok 5 písm. a) a b) ESĽP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000 ESĽP, *Taylor-Sabori/Spojené kráľovstvo*, č. 47114/99, 22. októbra 2002 ESĽP, *Peck/Spojené kráľovstvo*, č. 44647/98, 28. januára 2003 ESĽP, *Khelili/Švajčiarsko*, č. 16188/07, 18. októbra 2011 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987
Smernica o ochrane údajov, článok 6 ods. 1 písm. b)	**Zásada uvedenia a obmedzenia účelu**	Dohovor č. 108, článok 5 písm. b)
	Zásady kvality údajov:	
Smernica o ochrane údajov, článok 6 ods. 1 písm. c)	**Relevantnosť údajov**	Dohovor č. 108, článok 5 písm. c)
Smernica o ochrane údajov, článok 6 ods. 1 písm. d)	**Presnosť údajov**	Dohovor č. 108, článok 5 písm. d)

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov, článok 6 ods. 1 písm. e)	Obmedzené uchovávanie údajov	Dohovor č. 108, článok 5 písm. e)
Smernica o ochrane údajov, článok 6 ods. 1 písm. e)	Výnimka pre vedecký výskum a štatistiku	Dohovor č. 108, článok 9 ods. 3
Smernica o ochrane údajov, článok 6 ods. 1 písm. a)	Zásada prijateľného spracovania	Dohovor č. 108, článok 5 písm. a) ESĽP, *Haralambie/Rumunsko*, č. 21737/03, 27. októbra 2009 ESĽP, *K. H. a iní/Slovensko*, č. 32881/04, 6. novembra 2009
Smernica o ochrane údajov, článok 6 ods. 2	Zásada zodpovednosti	

Zásady stanovené v článku 5 dohovoru č. 108 zhŕňajú podstatu európskych právnych predpisov o ochrane údajov. Tieto zásady sú uvedené aj v článku 6 smernice o ochrane údajov ako východisko pre podrobnejšie ustanovenia v nasledujúcich článkoch smernice. Každý ďalší právny predpis o ochrane údajov na úrovni Rady Európy alebo EÚ musí byť v súlade s uvedenými zásadami a tieto zásady sa musia zohľadniť pri výklade následných právnych predpisov v oblasti ochrany údajov. Výnimky z uvedených hlavných zásad alebo ich obmedzenia môžu byť prijaté na vnútroštátnej úrovni[107], musia byť stanovené zákonom, musia mať legitímny cieľ a musia byť nevyhnutné v demokratickej spoločnosti. Je nutné, aby boli splnené všetky tri podmienky.

3.1. Zásada zákonného spracúvania

Hlavné body

- V záujme pochopenia zásady zákonného spracúvania sa treba zamerať na podmienky zákonných obmedzení práva na ochranu údajov z hľadiska článku 52 ods. 1 charty a požiadaviek na oprávnené zasahovanie podľa článku 8 ods. 2 EDĽP.
- Z týchto ustanovení vyplýva, že spracúvanie osobných údajov je zákonné len vtedy, keď:

107 Dohovor č. 108, článok 9 ods. 2; smernica o ochrane údajov, článok 13 ods. 2.

- je v súlade s právnymi predpismi;
- má legitímny účel;
- je nevyhnutné v demokratickej spoločnosti na dosiahnutie legitímneho účelu.

Zásada zákonného spracúvania je prvou zásadou uvedenou **v právnych predpisoch EÚ aj právnych predpisoch Rady Európy o ochrane údajov**. Je takmer rovnakým spôsobom vyjadrená v článku 5 dohovoru č. 108 a v článku 6 smernice o ochrane údajov.

Ani jedno z uvedených ustanovení neobsahuje vymedzenie pojmu „zákonné spracúvanie". Aby sme porozumeli tomuto právnickému termínu, musíme sa zmieniť o oprávnenom zásahu podľa EDĽP, ako ho vykladá judikatúra ESĽP, a podmienkach zákonných obmedzení podľa článku 52 charty.

3.1.1. Požiadavky na oprávnený zásah podľa EDĽP

Spracovanie osobných údajov môže predstavovať zásah do práva na rešpektovanie súkromného života dotknutej osoby. Právo na rešpektovanie súkromného života nie je absolútnym právom, ale musí byť vyvážené a zosúladené s ďalšími legitímnymi záujmami buď iných osôb (súkromné záujmy), alebo spoločnosti ako celku (verejné záujmy).

Zásah zo strany štátu je oprávnený za nasledujúcich okolností:

Súlad s právnymi predpismi

Podľa judikatúry ESĽP je zásah v súlade s právnymi predpismi vtedy, keď je založený na ustanovení vnútroštátneho právneho poriadku s určitými vlastnosťami. Príslušný právny predpis musí „byť prístupný dotknutým osobám a predvídateľný z hľadiska dôsledkov"[108]. Právny predpis je predvídateľný, ak „je formulovaný dostatočne presne na to, aby umožnil jednotlivcovi (podľa potreby s príslušným poradenstvom) reguláciu jeho správania"[109]. „Stupeň presnosti požadovaný v tejto súvislosti podľa zákona bude závisieť od konkrétneho predmetu"[110].

108 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 iní/Moldavsko*, č. 25198/02, 10. februára 2009, bod 50.

109 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 iní/Spojené kráľovstvo*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 a 7113/75, 25. marca 1983, bod 88.

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

Príklad: ESĽP vo veci *Rotaru/Rumunsko*[111] zistil porušenie článku 8 EDĽP, keďže v rumunských právnych predpisoch sa umožňoval zber, zaznamenávanie a archivovanie utajených súborov informácií týkajúcich sa národnej bezpečnosti, pričom sa v nich neukladali obmedzenia na vykonávanie týchto právomocí, ktoré záviseli od vlastného uváženia orgánov. Napríklad vo vnútroštátnych právnych predpisoch 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. Na základe uvedených nedostatkov súd dospel k záveru, že vnútroštátne právne predpisy nie sú v súlade s požiadavkou predvídateľnosti podľa článku 8 EDĽP a že došlo k porušeniu uvedeného článku.

Príklad: Vo veci *Taylor-Sabori/Spojené kráľovstvo*[112] 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 paralelných písomne zaznamenaných 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 právnym poriadkom". ESĽP dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

Dosahovanie legitímneho cieľa

Legitímnym cieľom môže byť niektorý z uvedených verejných záujmov alebo práva a slobody iných.

Príklad: Sťažovateľ vo veci *Peck/Spojené kráľovstvo*[113] sa pokúsil spáchať samovraždu tak, že si na ulici podrezal zápästia, pričom nevedel o tom, že tento pokus zaznamenala priemyselná kamera. Príslušník polície, ktorý sledoval záznamy kamerového systému, sťažovateľa zachránil a policajný orgán následne poskytol záznam kamerového systému médiám, ktoré ho zverejnili

111 ESĽP, *Rotaru/Rumunsko* [VK], č. 28341/95, 4. mája 2000, bod 57; pozri tiež ESĽP, *Združenie pre európsku integráciu a ľudské práva a Ekimdžiev/Bulharsko*, č. 62540/00, 28. júna 2007; ESĽP, *Šimovolos/Rusko*, č. 30194/09, 21. júna 2011 a ESĽP, *Vetter/Francúzsko*, č. 59842/00, 31. mája 2005.

112 ESĽP, *Taylor-Sabori/Spojené kráľovstvo*, č. 47114/99, 22. októbra 2002.

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

s odokrytou tvárou sťažovateľa. ESĽP dospel k záveru, že neexistovali žiadne relevantné ani dostatočné dôvody, ktoré by oprávňovali orgány priamo zverejniť záznam bez súhlasu sťažovateľa alebo skrytia jeho totožnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

Nevyhnutnosť 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“[114].

Príklad: Vo veci *Khelili/Švajčiarsko*[115] polícia počas policajnej kontroly zistila, že sťažovateľka má pri sebe navštívenky, na ktorých bolo napísané: „Milá a pekná žena na prahu štyridsiatky by sa rada zoznámila s mužom, ktorý by si s ňou čas od času zašiel na pohárik alebo do spoločnosti. Tel. č. [...].“ Sťažovateľka tvrdila, že po nájdení navštíveniek polícia zapísala jej meno do registra prostitútok, čo je zamestnanie, ktoré ona trvale popiera. Sťažovateľka požadovala odstránenie slova „prostitútka“ z policajných záznamov. ESĽP v zásade uznal, že uchovávanie osobných údajov jednotlivca na základe skutočnosti, že daná osoba 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 EDĽP. Súd zohľadnil skutočnosť, že úrady mali overiť presnosť uchovávaných údajov o sťažovateľke, ako aj závažnosť zásahu do jej práv a uzniesol sa, že dlhoročný zápis slova „prostitútka“ v policajných spisoch nebol nevyhnutný v demokratickej spoločnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

Príklad: ESĽP vo veci *Leander/Švédsko*[116] rozhodol, že bezpečnostná 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, ESĽP dospel k záveru, že švédsky systém previerok zamestnancov spĺňa požiadavky článku 8 ods. 2

114 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. Marca 1987, bod 58.

115 ESĽP, *Khelili/Švajčiarsko*, č. 16188/07, 18. Októbra 2011.

116 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. Marca 1987, body 59 a 67.

EDĽP. Vzhľadom na široké uznanie systému mal žalovaný štát nárok domnievať sa, že v prípade sťažovateľa záujmy národnej bezpečnosti prevažujú nad individuálnymi záujmami. Súd dospel k záveru, že nedošlo k porušeniu článku 8 EDĽP.

3.1.2. Podmienky zákonných obmedzení podľa charty

Štruktúra a znenie charty sa líšia od EDĽP. V charte sa nepíše o zásahoch 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;
- rešpektujú podstatu práva na ochranu údajov;
- sú nevyhnutné podľa zásady proporcionality;
- zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou alebo sú potrebné na ochranu práv a slobôd iných.

Príklady: SDEÚ vo veci *Volker a Markus Schecke*[117] dospel k záveru, že Rada a Komisia 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, nedodržali obmedzenia vyplývajúce zo zásady proporcionality.

Preto SDEÚ považoval za nutné vyhlásiť neplatnosť určitých ustanovení nariadenia Rady (ES) č. 1290/2005 a neplatnosť nariadenia č. 259/2008 v celom jeho rozsahu[118].

117 SDEÚ, spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen*, 9. Novembra 2010, body 89 a 86.

118 Nariadenie Rady (ES) č. 1290/2005 z 21. júna 2005 o financovaní spoločnej poľnohospodárskej politiky, Ú. v. EÚ L 209, 2005 a 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 prijímateľoch pomoci zo zdrojov Európskeho poľnohospodárskeho záručného fondu (EPZF) a Európskeho poľnohospodárskeho fondu pre rozvoj vidieka (EPFRV), Ú. v. EÚ L 76, 2008.

Napriek odlišnému zneniu sa podmienky zákonného spracúvania stanovené v článku 52 ods. 1 charty podobajú podmienkam stanoveným v článku 8 ods. 2 EDĽP. Treba pochopiť, že podmienky vymenované v článku 52 ods. 1 sú v súlade s podmienkami uvedenými v článku 8 ods. 2 EDĽP, keďže v článku 52 ods. 3 charty sa v prvej vete uvádza, 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".

Podľa poslednej vety článku 52 ods. 3 „toto ustanovenie nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany týchto práv". Po porovnaní článku 8 ods. 2 EDĽP a prvej vety článku 52 ods. 3 to môže znamenať len toľko, že podmienky oprávneného zásahu podľa článku 8 ods. 2 EDĽP predstavujú minimálne požiadavky na zákonné obmedzenia práva na ochranu údajov podľa charty. Z uvedeného vyplýva, že zákonné spracúvanie osobných údajov podľa právnych predpisov EÚ si vyžaduje, aby boli splnené aspoň požiadavky článku 8 ods. 2 EDĽP, pričom sa však v právnych predpisoch EÚ môžu v osobitných prípadoch stanoviť dodatočné požiadavky.

Zhoda zásady zákonného spracúvania podľa právnych predpisov EÚ s relevantnými ustanoveniami EDĽP je zdôraznená aj v článku 6 ods. 3 ZEÚ, v ktorom sa uvádza, že „základné práva tak, ako sú zaručené Európskym dohovorom o ochrane ľudských práv a základných slobôd [...] predstavujú všeobecné zásady práva Únie".

3.2. Zásada uvedenia a obmedzenia účelu

Hlavné body

- Pred začiatkom spracúvania údajov musí byť viditeľne vymedzený účel spracúvania.
- Podľa právnych predpisov EÚ musí byť účel spracúvania výslovne definovaný, v právnych predpisoch Rady Európy sa táto otázka ponecháva na vnútroštátne právne predpisy.
- Spracúvanie na nevymedzené účely nie je v súlade s právnymi predpismi o ochrane údajov.
- Ďalšie použitie údajov na iný účel si vyžaduje dodatočný právny základ v tom prípade, že nový účel spracúvania nie je zlučiteľný s pôvodným účelom.
- Prenos údajov tretím stranám je novým účelom vyžadujúcim si dodatočný právny základ.

Zásada uvedenia a obmedzenia účelu v podstate znamená, že legitímnosť spracovania osobných údajov bude závisieť od účelu spracovania[119]. Účel musí špecifikovať a vyhlásiť prevádzkovateľ pred začiatkom spracúvania údajov[120]. **Podľa právnych prepisov EÚ** to prevádzkovateľ musí urobiť buď formou vyhlásenia (inými slovami oznámením) príslušnému dozornému orgánu, alebo aspoň formou interného dokumentu, ktorý musí sprístupniť kontrole zo strany dozorného orgánu a ku ktorému musí umožniť prístup dotknutej osobe.

Spracúvanie osobných údajov na nevymedzené alebo neobmedzené účely je nezákonné.

Každý nový účel spracúvania údajov musí mať vlastný právny základ a nemôže sa opierať o skutočnosť, že údaje boli pôvodne nadobudnuté alebo spracované na iný legitímny účel. Na druhej strane je legitímne spracúvanie obmedzené na svoj pôvodný uvedený účel a každý nový účel spracúvania si bude vyžadovať samostatný nový právny základ. Zvlášť pozorne treba zvážiť zverejnenie údajov tretím stranám, keďže zverejnenie zvyčajne predstavuje nový účel, a preto si vyžaduje iný právny základ, ako je právny základ zberu údajov.

Príklad: Letecká spoločnosť zbiera údaje svojich cestujúcich pri rezerváciách, aby mohla riadne prevádzkovať lety. Zozbierané údaje bude potrebovať: na určenie čísel sedadiel cestujúcich, najmä v prípade fyzických obmedzení, napríklad u osôb na invalidnom vozíku, a v súvislosti s osobitnými požiadavkami na stravu (napríklad kóšer alebo halal). Ak letecké spoločnosti musia preniesť tieto údaje uvedené v zázname o cestujúcom (PNR) imigračným orgánom na pristávacom letisku, údaje sú následne použité na účely imigračnej kontroly, teda účely, ktoré sa odlišujú od pôvodného účelu zberu údajov. Prenos uvedených údajov imigračným orgánom si bude teda vyžadovať nový a samostatný právny základ.

V dohovore č. 108 a smernici o ochrane údajov sa pri posudzovaní rozsahu a obmedzení konkrétneho účelu opiera o pojem zlučiteľnosti: použitie údajov na zlučiteľné účely je povolené na základe pôvodného právneho základu. Obsah pojmu „zlučiteľný“ však nie je vymedzený a ponecháva sa voľnému výkladu v jednotlivých prípadoch.

119 Dohovor č. 108, článok 5 písm. b); smernica o ochrane údajov, článok 6 ods. 1 písm. b).

120 Pozri tiež: pracovná skupina zriadená podľa článku 29 (2013), *stanovisko 03/2013 k obmedzeniu účelu*, WP 203, Brusel, 2. apríla 2013.

Príklad: Predaj údajov o zákazníkoch spoločnosti Sunshine, ktoré spoločnosť Sunshine nadobudla v rámci riadenia vzťahov so zákazníkmi, spoločnosti Moonlight (spoločnosť, ktorá sa venuje priamemu marketingu), ktorá chce tieto údaje použiť ako pomôcku pri marketingových kampaniach tretích spoločností, je nový účel, ktorý nie zlučiteľný s riadením vzťahov so zákazníkmi – pôvodným účelom zberu údajov o zákazníkoch zo strany spoločnosti Sunshine. Predaj údajov spoločnosti Moonlight 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 prijíma ako zlučiteľný účel.

V smernici o ochrane údajov sa výslovne uvádza, že „ďalšie spracovanie údajov pre historické, štatistické alebo vedecké účely sa nepovažuje za nezlučiteľné, pod podmienkou, že členské štáty zabezpečia primerané bezpečnostné opatrenia“[121].

Príklady: 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.

Ak sa takéto údaje majú preniesť tretej strane – spoločnosti Starlight – výlučne na štatistické účely, prenos by bol prípustný bez dodatočného právneho základu, ale len pod podmienkou prijatia príslušných záruk, napríklad skrytia totožnosti dotknutých osôb, keďže totožnosť zvyčajne nie je na štatistické účely potrebná.

3.3. Zásady kvality údajov

Hlavné body

- Zásadu kvality údajov musí prevádzkovateľ uplatňovať pri všetkých operáciách spracúvania.

121 Príkladom takýchto vnútroštátnych ustanovení je rakúsky zákon o ochrane údajov (*Datenschutzgesetz*), Spolkový právny úradný vestník I č. 165/1999, odsek 46, dostupný v anglickom jazyku na adrese: www.dsk.gv.at/DocView.axd?CobId=41936.

- Podľa zásady obmedzeného uchovávania údajov je nutné čo najskôr odstrániť údaje, ktoré už nie sú potrebné na účely, na ktoré boli zozbierané.
- Výnimky zo zásady obmedzeného uchovávania údajov musia byť stanovené zo zákona a vyžadujú osobitné záruky na ochranu dotknutých osôb.

3.3.1. Zásada relevantnosti údajov

Spracúvajú sa len také údaje, ktoré sú „adekvátne, relevantné a nie nadbytočné vzhľadom na účely, na ktoré sa uchovávajú“[122]. Kategórie údajov vybraných na spracovanie musia byť nutné z hľadiska vyhláseného celkového cieľa operácií spracovania a prevádzkovateľ by mal prísne obmedziť zber údajov na tie informácie, ktoré sú priamo relevantné pre špecifický účel spracovania.

V súčasnej spoločnosti má zásada relevantnosti údajov dodatočný aspekt: ak sa uplatní špeciálna technológia na zvyšovanie súkromia, niekedy je možné úplne sa vyhnúť použitiu osobných údajov alebo použiť pseudonymizované údaje, čo je riešenie, ktoré vyhovuje zásadám ochrany súkromia. To je vhodné najmä v rozsiahlejších systémoch spracúvania.

Príklad: Mestská rada ponúka pravidelným používateľom systému mestskej hromadnej dopravy čipovú kartu za určitý poplatok. Meno používateľa je napísané na povrchu karty a uvedené 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 nerešpektuje optimálne zásadu relevantnosti: 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 nezaznamenával, kto použil aký dopravný prostriedok a kedy. Nezbierali by sa žiadne osobné údaje, čo predstavuje optimálne riešenie v zmysle zásady relevantnosti, keďže konečným dôsledkom tejto zásady je povinnosť minimalizovať zber údajov.

122 Dohovor č. 108, článok 5 písm. c) a smernica o ochrane údajov, článok 6 ods. 1 písm. c).

3.3.2. Zásada presnosti údajov

Prevádzkovateľ, ktorý uchováva osobné údaje, musí pred ich použitím s primeranou určitosťou zabezpečiť, že sú presné a aktuálne.

Povinnosť zaistiť presnosť údajov treba chápať v súvislosti s účelom ich spracovania.

Príklad: Nábytkársky podnik zozbieral údaje o totožnosti a adresách zákazníkov, aby im mohol vystaviť faktúru. O šesť mesiacov neskôr chce tento podnik začať marketingovú kampaň a rád by kontaktoval bývalých zákazníkov. Z uvedeného dôvodu má v úmysle nahliadnuť do registra obyvateľstva, ktorý by mal obsahovať aktuálne adresy, keďže občania sú zo zákona povinní informovať register o svojej aktuálnej adrese. Prístup k údajom registra obyvateľov je obmedzený na osoby a subjekty, ktoré môžu uviesť oprávnený dôvod.

V uvedenej situácii spoločnosť nemôže argumentovať tým, že údaje musia byť presné a aktuálne a tvrdiť, že je oprávnená získať nové adresy všetkých bývalých zákazníkov z registra obyvateľov. Údaje boli zozbierané v rámci fakturácie a na tento účel je relevantná adresa v čase predaja. Neexistuje žiadny právny základ pre zber nových adries, keďže marketing nie je záujem, ktorý by mal prednosť pred právom na ochranu údajov, a preto nemôže oprávniť prístup k údajom v registri.

Môžu sa vyskytnúť aj prípady, keď je aktualizácia uložených údajov právne zakázaná, keďže účel uchovávania údajov je v prvom rade zdokumentovať udalosti.

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

Na druhej strane existujú situácie, v ktorých je pravidelná kontrola presnosti údajov (vrátane aktualizácií) absolútne nevyhnutná z dôvodu možnej škody, ktorá by mohla vzniknúť dotknutej osobe v prípade, že by údaje zostali nepresné.

Príklad: Ak chce niekto uzatvoriť zmluvu bankou, poskytovateľ zvyčajne skontroluje solventnosť možného zákazníka. Na tento účel existujú špeciálne databázy obsahujúce údaje o úverovej histórii súkromných jednotlivcov. Keby takáto

databáza obsahovala nesprávne alebo zastarané údaje o jednotlivcovi, príslušnej osobe by mohli vzniknúť problémy. Prevádzkovatelia takýchto databáz preto musia vynaložiť osobitné úsilie na dodržanie zásady presnosti.

Okrem toho údaje, ktoré nesúvisia s faktami, ale s domnienkami, napríklad v rámci trestných stíhaní, sa môžu zbierať a uchovávať len dovtedy, kým prevádzkovateľ má právny základ na zbieranie takýchto informácií a je dostatočne oprávnený na formulovanie podozrení.

3.3.3. Zásada obmedzeného uchovávania údajov

V článku 6 ods. 1 písm. e) smernice o ochrane údajov sa podobne ako v článku 5 písm. e) dohovoru č. 108 požaduje, aby členské štáty zabezpečili, že osobné údaje budú „udržiavané vo forme, ktorá umožňuje identifikáciu osôb pracujúcich s údajmi počas obdobia ktoré je nevyhnutné na účely, pre ktoré boli údaje zhromažďované, alebo pre ktoré sú ďalej spracovávané“. Keď údaje poslúžia na stanovený účel, musia sa vymazať.

ESĽP vo veci *S. a Marper* dospel k záveru, že v rámci základných zásad relevantných nástrojov Rady Európy, ako aj v právnych predpisoch a praxi ďalších zmluvných strán sa požaduje, aby uchovávanie údajov bolo primerané účelu ich zberu a obmedzené v čase, predovšetkým v policajnom sektore[123].

Časové obmedzenie uchovávania osobných údajov platí nielen pre údaje uchovávané v podobe, ktorá umožňuje identifikáciu dotknutých osôb. Zákonné uchovávanie údajov, ktoré už nie sú potrebné, by sa mohlo dosiahnuť ich anonymizáciou alebo pseudonymizáciou.

Zo zásady obmedzeného uchovávania údajov je v smernici o ochrane údajov výslovne vyňaté uchovávanie údajov na budúce vedecké, historické alebo štatistické použitie[124]. Takéto nepretržité uchovávanie a používanie osobných údajov však musia sprevádzať osobitné záruky vyplývajúce z vnútroštátnych právnych predpisov.

123 ESĽP, *S. a Marper/Spojené kráľovstvo*, č. 30562/04 a 30566/04, 4. decembra 2008; pozri tiež napríklad ESĽP, *M.M./Spojené kráľovstvo*, č. 24029/07, 13. novembra 2012.

124 Smernica o ochrane údajov, článok 6 ods. 1 písm. e).

3.4. Zásada prijateľného spracovania

Hlavné body

- Prijateľné spracovanie znamená transparentnosť spracovania, a to najmä voči dotknutým osobám.
- Prevádzkovatelia musia informovať dotknuté osoby pred spracovaním údajov týchto osôb aspoň o účele spracovania a totožnosti a adrese prevádzkovateľa.
- Nie je prípustné žiadne tajné ani skryté spracovanie osobných údajov, okrem prípadov, keď ho osobitne povoľujú právne predpisy.
- Dotknuté osoby majú právo na prístup k svojim údajom bez ohľadu na to, kde sa tieto údaje spracúvajú.

Zásada prijateľného spracovania upravuje predovšetkým vzťah medzi prevádzkovateľom a dotknutou osobou.

3.4.1. Transparentnosť

Touto zásadou sa stanovuje povinnosť prevádzkovateľa informovať dotknuté osoby o tom, akým spôsobom sa používajú ich údaje.

Príklad: Sťažovateľ vo veci *Haralambie/Rumunsko*[125] požadoval prístup k spisu, ktorý o ňom uchovávala tajná služba, orgány však vyhoveli tejto žiadosti až o päť rokov neskôr. ESĽP opätovne pripomenul, že jednotlivci, o ktorých verejné orgány vedú osobné spisy, majú životný záujem na sprístupnení týchto spisov. Orgány sú povinné zaistiť efektívny spôsob získania prístupu k takýmto informáciám. ESĽP sa domnieval, že ani množstvo prenesených spisov, ani nedostatky v systéme archivácie neoprávňujú k päťročnému zdržaniu pri riešení 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 EDĽP.

Operácie spracovania musia byť dotknutým osobám vysvetlené zrozumiteľným spôsobom, ktorým sa zaručí, že dotknuté osoby chápu, čo sa bude diať s ich údajmi.

125 ESĽP, *Haralambie/Rumunsku*, č. 21737/03, 27. októbra 2009.

Dotknutá osoba má takisto právo, aby ju prevádzkovateľ na jej žiadosť informoval, či sa jej údaje spracúvajú a ak áno, o ktoré údaje ide.

3.4.2. Získanie dôvery

Prevádzkovatelia by mali dotknutým osobám a všeobecne verejnosti doložiť, že budú údaje spracúvať zákonným a transparentným spôsobom. Operácie spracúvania sa nesmú vykonávať tajne a nesmú mať nepredvídateľné negatívne následky. Prevádzkovatelia by mali zaistiť, aby zákazníci, klienti alebo občania boli informovaní o použití svojich údajov. Prevádzkovatelia musia v maximálnej možnej miere konať tak, aby bez meškania vyhoveli žiadostiam dotknutých osôb, predovšetkým vtedy, keď súhlas dotknutej osoby predstavuje právny základ spracovania údajov.

Príklad: Vo veci *K. H. a iní/Slovensko*[126] sa sťažovalo osem žien rómskeho pôvodu, ktoré boli počas tehotenstva a pri pôrode ošetrené 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 nemocniciam, aby povolili sťažovateľkám a ich zástupcom nahliadnutie do lekárskych záznamov a vypracovanie písomného výťahu z nich, ale zamietli ich žiadosť o vytvorenie fotokópií dokumentov, údajne preto, aby zabránili ich zneužitiu. Povinnosti štátov konať vyplývajúce z článku 8 EDĽP 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 sťažovateliek domáce súdy zdôvodnili zákaz vyhotovenia fotokópií lekárskych záznamov 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 lekárskemu 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 sťažovateliek k informáciám, ktoré sa týkajú ich zdravia. Súd dospel k záveru, že došlo k porušeniu článku 8.

Pokiaľ ide o internetové služby, funkcie systémov na spracúvanie údajov musia dotknutým osobám umožňovať, aby skutočne porozumeli tomu, čo sa deje s ich údajmi.

126 ESĽP, *K.H.a iní/Slovensko*, č. 32881/04, 6. novembra 2009.

Prijateľné spracovanie takisto znamená, že prevádzkovateľ je ochotný urobiť viac, ako predpisujú povinné minimálne právne požiadavky na služby dotknutým osobám, ak to budú vyžadovať legitímne záujmy dotknutej osoby.

3.5. Zásada zodpovednosti

Hlavné body

- Zodpovednosť si vyžaduje, aby prevádzkovatelia aktívne vykonávali opatrenia na podporu a zabezpečenie ochrany údajov pri ich spracúvaní.
- Prevádzkovatelia sú zodpovední za súlad operácií spracovania s právnymi predpismi o ochrane údajov.
- Prevádzkovatelia by mali byť schopní kedykoľvek preukázať súlad s ustanoveniami o ochrane údajov dotknutým osobám, širokej verejnosti a dozorným orgánom.

Organizácia pre hospodársku spoluprácu a rozvoj (OECD) prijala v roku 2013 vlastné usmernenia, v ktorých zdôraznila, že prevádzkovatelia majú v praxi dôležitú úlohu pri ochrane údajov. V usmerneniach je rozpracovaná zásada zodpovednosti v takom rozsahu, že „prevádzkovateľ by mal byť zodpovedný za súlad s opatreniami, ktoré zaisťujú realizáciu uvedených [vecných] zásad“[127].

Zatiaľ čo v dohovore č. 108 sa vôbec neodkazuje na zodpovednosť prevádzkovateľov a v podstate sa v ňom táto otázka ponecháva na vnútroštátne právne predpisy, v článku 6 ods. 2 smernice o ochrane údajov sa uvádza, že prevádzkovateľ by mal zaistiť súlad so zásadami týkajúcimi sa kvality údajov zahrnutými do odseku 1.

Príklad: Legislatívnym príkladom, ktorý zdôrazňuje zásadu zodpovednosti, je zmena smernice 2002/58/ES o súkromí v elektronických komunikáciách[128]. Podľa článku 4 zmeneného znenia smernice sa ukladá povinnosť vykonávať

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

128 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 2009 L 337, s. 11.

bezpečnostnú politiku, a to „zabezpečenie vykonávania bezpečnostnej politiky vo vzťahu k spracovaniu osobných údajov“. Pokiaľ ide o bezpečnostné ustanovenia uvedenej smernice, zákonodarca rozhodol, že je nevyhnutne potrebné uviesť výslovnú požiadavku vypracovať a vykonávať bezpečnostnú politiku.

Podľa stanoviska pracovnej skupiny zriadenej podľa článku 29[129] je podstatou zodpovednosti povinnosť prevádzkovateľa:

- zaviesť opatrenia, ktoré by (za normálnych okolností) zaručili dodržiavanie pravidiel ochrany údajov v kontexte operácií spracúvania;

- vypracovať dokumenty, ktoré dotknutým osobám a dozorným orgánom potvrdia, aké opatrenia boli zavedené na dosiahnutie súladu s právnymi predpismi o ochrane údajov.

Zásada zodpovednosti si teda vyžaduje, aby prevádzkovatelia pasívne nečakali, až ich dotknuté osoby alebo dozorné orgány upozornia na nedostatky, ale aby aktívne preukázali súlad s právnymi predpismi.

129 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko č. 3/2007 k zásade zodpovednosti*, WP 173, Brusel, 13. júla 2010.

4

Pravidlá európskeho práva v oblasti ochrany údajov

EÚ	Zahrnuté otázky	Rada Európy
Pravidlá zákonného spracúvania údajov, ktoré nie sú citlivé		
Smernica o ochrane údajov, článok 7 písm. a)	**Súhlas**	Odporúčanie o profilovaní, článok 3.4 písm. b) a článok 3.6
Smernica o ochrane údajov, článok 7 písm. b)	**(Predzmluvný) zmluvný vzťah**	Odporúčanie o profilovaní, článok 3.4 písm. b)
Smernica o ochrane údajov, článok 7 písm. c)	**Právne povinnosti prevádzkovateľa**	Odporúčanie o profilovaní, článok 3.4 písm. a)
Smernica o ochrane údajov, článok 7 písm. d)	**Životné záujmy dotknutých osôb**	Odporúčanie o profilovaní, článok 3.4 písm. b)
Smernica o ochrane údajov, článok 7 písm. e) a článok 8 ods. 4 SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland* , 16. decembra 2008	**Verejný záujem a uplatňovanie oficiálneho poverenia**	Odporúčanie o profilovaní, článok 3.4 písm. b)
Smernica o ochrane údajov, článok 7 písm. f), článok 8 ods. 2 a 3 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	**Legitímne záujmy iných**	Odporúčanie o profilovaní, článok 3.4 písm. b)
Pravidlá zákonného spracúvania citlivých údajov		
Smernica o ochrane údajov, článok 8 ods. 1	**Všeobecný zákaz spracovania**	Dohovor č. 108, článok 6

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov, článok 8 ods. 2 až 4	Výnimky zo všeobecného zákazu	Dohovor č. 108, článok 6
Smernica o ochrane údajov, článok 8 ods. 5	Spracúvanie údajov o odsúdení (v trestných veciach)	Dohovor č. 108, článok 6
Smernica o ochrane údajov, článok 8 ods. 7	Identifikačné čísla spracúvania	
Pravidlá bezpečného spracúvania		
Smernica o ochrane údajov, článok 17 písm. a)	Povinnosť zabezpečiť bezpečnosť spracovania	Dohovor č. 108, článok 7
		ESĽP, *I./Fínsko*, č. 20511/03, 17. júla 2008
Smernica o súkromí v elektronických komunikáciách, článok 4 ods. 2	Oznámenie o porušení ochrany údajov	
Smernica o ochrane údajov, článok 16	Povinnosť dôvernosti	
Pravidlá transparentnosti spracúvania		
	Transparentnosť vo všeobecnosti	Dohovor č. 108, článok 8 písm. a)
Smernica o ochrane údajov, články 10 a 11	Informácie	Dohovor č. 108, článok 8 písm. a)
Smernica o ochrane údajov, články 10 a 11	Výnimky z povinnosti informovať	Dohovor č. 108, článok 9
Smernica o ochrane údajov, články 18 a 19	Oznámenie	Odporúčanie o profilovaní, článok 9.2 písm. a)
Pravidlá podpory súladu		
Smernica o ochrane údajov, článok 20	Predbežná kontrola	
Smernica o ochrane údajov, článok 18 ods. 2	Zodpovedné osoby	Odporúčanie o profilovaní, článok 8.3
Smernica o ochrane údajov, článok 27	Kódexy správania	

Zásady majú nevyhnutne všeobecnú povahu. Pri ich uplatňovaní v konkrétnych situáciách sa ponecháva určitý priestor pre výklad a výber prostriedkov. **V rámci právnych predpisov Rady Európy** je na zmluvných stranách dohovoru č. 108, aby tento priestor pre výklad ozrejmili vo vnútroštátnych právnych predpisoch. Situácia v rámci **právnych predpisov EÚ** je iná: v záujme uplatnenia ochrany údajov na vnútornom trhu sa považovalo za nevyhnutné stanoviť podrobnejšie pravidlá už na úrovni EÚ s cieľom harmonizovať úroveň ochrany údajov vo vnútroštátnych právnych poriadkoch členských štátov. V smernici o ochrane údajov sa v rámci súboru zásad zahrnutých do článku 6 stanovuje úroveň podrobných pravidiel, ktoré sa musia dôsledne dodržiavať v rámci vnútroštátnych právnych predpisov. Nasledujúce poznámky k podrobným pravidlám ochrany údajov na európskej úrovni sú preto venované prevažne právu EÚ.

4.1. Pravidlá zákonného spracúvania

Hlavné body

- Osobné údaje sa spracúvajú zákonne vtedy, keď:
  - je spracúvanie založené na súhlase dotknutej osoby alebo
  - sa spracúvanie údajov vyžaduje v rámci životných záujmov dotknutých osôb, alebo
  - sú dôvodom spracúvania legitímne záujmy iných, ale len do tej miery, ak nie sú prevýšené záujmami na ochranu základných práv dotknutých osôb.
- Na zákonné spracúvanie citlivých osobných údajov sa vzťahuje osobitný a prísnejší režim.

Smernica o ochrane údajov obsahuje dva rôzne súbory pravidiel zákonného spracúvania údajov: jeden pre údaje, ktoré nie sú citlivé (v článku 7) a druhý pre citlivé údaje (v článku 8).

4.1.1. Pravidlá zákonného spracúvania údajov, ktoré nie sú citlivé

V kapitole II smernice 95/46 s názvom Všeobecné nariadenia týkajúce sa zákonnosti spracovania osobných údajov sa stanovuje, že okrem výnimiek povolených v článku 13 musí byť každé spracúvanie osobných údajov v súlade so zásadami týkajúcimi sa kvality údajov uvedenými v článku 6 smernice o ochrane údajov a, ďalej s jedným z kritérií legitímnosti spracovania údajov uvedených v článku 7[130]. Ide o prípady, ktoré spracúvania osobných údajov, ktoré nie sú citlivé, robia legitímnym.

Súhlas

V rámci právnych predpisov Rady Európy sa pojem súhlas neuvádza ani v článku 8 EDĽP, ani v dohovore č. 108. Obsahuje ho však judikatúra ESĽP a niekoľko odporúčaní Rady Európy. **V rámci právnych predpisov EÚ** súhlas ako základ

130 SDEÚ, spojené veci C-465/00, C-138/01 a C-139/01 *Österreichischer Rundfunk a iní*, 20. mája 2003, bod 65; SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland*, 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 (FECEMD)/Administración del Estado*, 24. novembra 2011, bod 26.

legitímneho spracovania údajov je pevne stanovený v článku 7 písm. a) smernice o ochrane údajov a je takisto výslovne uvedený v článku 8 charty.

Zmluvný vzťah

Ďalším základom pre legitímne spracúvanie osobných údajov **podľa právnych predpisov EÚ** je ustanovenie uvedené v článku 7 písm. b) smernice o ochrane údajov, podľa ktorého je spracovanie legitímne, ak je „nevyhnutné pre výkon zmluvy, ktorej je osoba pracujúca s údajmi zainteresovanou stranou". Toto ustanovenie zahŕňa tiež vzťahy pred uzatvorením zmluvy. Napríklad, strana má v úmysle uzatvoriť zmluvu, zatiaľ to však neurobila, pravdepodobne preto, lebo ešte musí vykonať niektoré kontroly. Ak jedna strana potrebuje spracovať údaje na tento účel, takéto spracovanie je legitímne vtedy, ak sa uskutoční, „aby sa vykonali opatrenia na požiadanie osoby pracujúcej s údajmi pred uzatvorením zmluvy".

V právnych predpisoch Rady Európy, v článku 8 ods. 2 EDĽP sa za dôvod legitímneho zásahu do práva na ochranu údajov pokladá „[ochrana] práv a slobôd iných".

Právne povinnosti prevádzkovateľa

V právnych predpisoch EÚ sa výslovne uvádza ďalšie kritérium legitímnosti spracúvania údajov, a to v prípade, že „spracovanie je nevyhnutné na vyhovenie právnemu záväzku, ktorého subjektom je kontrolór" (článok 7 písm. c) smernice o ochrane údajov). Toto ustanovenie sa vzťahuje na prevádzkovateľov pôsobiacich v súkromnom sektore, na zákonné povinnosti prevádzkovateľov vo verejnom sektore sa vzťahujú ustanovenia článku 7 písm. e) uvedenej smernice. Existuje veľa prípadov, v ktorých sú prevádzkovatelia v súkromnom sektore zo zákona povinní spracúvať údaje o iných, napríklad lekári alebo nemocnice majú zákonnú povinnosť uchovávať údaje o liečení pacientov niekoľko rokov, zamestnávatelia musia spracúvať údaje o svojich zamestnancoch z dôvodov sociálneho zabezpečenia a zdanenia a podnikatelia musia spracúvať údaje o svojich zákazníkoch z dôvodov zdanenia.

V súvislosti s povinným poskytovaním údajov o cestujúcich imigračným orgánom zo strany leteckých spoločností vzniká otázka, či právne povinnosti vyplývajúce zo *zahraničného* právneho poriadku môžu tvoriť právny základ pre spracúvanie údajov podľa právnych predpisov EÚ (tejto otázke sa podrobne venuje oddiel 6.2).

Právne povinnosti prevádzkovateľa slúžia ako základ pre legitímne spracúvanie údajov aj **v rámci právnych predpisov Rady Európy**. Ako sme už upozornili, právne

povinnosti prevádzkovateľa zo súkromného sektora predstavujú len jeden osobitný prípad legitímnych záujmov iných, ako sú uvedené v článku 8 ods. 2 EDĽP. Uvedený príklad sa teda týka aj právnych predpisov Rady Európy.

Životné záujmy dotknutých osôb

V rámci právnych predpisov EÚ sa v článku 7 písm. d) smernice o ochrane údajov stanovuje, že spracúvanie údajov je zákonné vtedy, keď „je nevyhnutné, aby sa ochránili životné záujmy osoby pracujúcej s údajmi". Tieto záujmy, ktoré úzko súvisia s prežitím dotknutej osoby, môžu byť základom legitímneho použitia údajov týkajúcich sa zdravia alebo napríklad údajov o nezvestných osobách.

V rámci právnych predpisov Rady Európy nie sú v článku 8 EDĽP životné záujmy dotknutej osoby uvedené ako dôvod legitímneho zásahu do práva na ochranu údajov. V niektorých odporúčaniach dopĺňajúcich dohovor č. 108 v konkrétnych oblastiach sa však životné záujmy dotknutých osôb výslovne uvádzajú ako základ legitímneho spracúvania údajov[131]. Je zrejmé, že životné záujmy dotknutej osoby sa výslovne predpokladajú v súbore dôvodov oprávňujúcich spracovanie údajov: ochrana základných práv by nikdy nemala ohroziť životné záujmy chránenej osoby.

Verejný záujem a uplatňovanie oficiálneho poverenia

Vzhľadom na viaceré možné spôsoby organizácie vecí verejných sa v článku 7 písm. e) smernice o ochrane údajov stanovuje, že osobné údaje môžu byť zákonne spracované, ak „spracovanie je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo v uplatňovaní oficiálneho poverenia zvereného kontrolórovi, alebo tretej strane, ktorej sa údaje odhalia [...]"[132].

Príklad: Vo veci *Huber/Bundesrepublik Deutschland*[133] požiadal pán Huber, rakúsky štátny príslušník bývajúci v Nemecku, Spolkový úrad pre migráciu a utečencov, aby odstránil údaje, ktoré sa ho týkajú, z centrálneho registra zahraničných štátnych príslušníkov („AZR"). 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

131 Odporúčanie o profilovaní, článok 3.4 písm. b).

132 Pozri tiež smernicu o ochrane údajov, odôvodnenie 32.

133 SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland*, 16. decembra 2008.

a stíhaní páchateľov trestnej činnosti alebo osôb, ktoré ohrozujú verejnú bezpečnosť. Súd, ktorý položil prejudiciálnu otázku, sa pýtal, či je spracovanie 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 najprv konštatoval, že podľa článku 7 písm. e) smernice je spracúvanie osobných údajov zákonné len vtedy, keď je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo pri uplatňovaní oficiálneho poverenia.

Podľa Súdneho dvora „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 95/46 [...] 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“[134].

Súdny dvor poznamenal, že právo občanov Únie na voľný pohyb na území členského štátu, ktorého daný občan nie je štátnym príslušníkom, nie je nepodmienené, ale môžu sa naň vzťahovať obmedzenia a podmienky uložené zmluvou a opatreniami, ktorých prostredníctvom nadobúda účinnosť. Takže 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. Súdny dvor dospel k záveru, že takýto systém spracovania 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. Keby 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) smernice 95/46/ES[135].

134 Tamtiež, bod 52.

135 Tamtiež, body 54, 58, 59, 66 až 68.

Pokiaľ ide o otázku používania údajov obsiahnutých v registri na účely boja proti trestnej činnosti, Súdny dvor uvádza, že tento cieľ nevyhnutne zahŕňa „stíhanie spáchaných trestných činov a priestupkov bez ohľadu na štátnu príslušnosť ich páchateľov". 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 toto ustanovenie (ako ho vykladá Súdny dvor) „bráni tomu, aby členský štát s cieľom boja proti trestnej činnosti zaviedol systém spracovávania osobných údajov týkajúcich sa len občanov Únie, ktorí nie sú jeho štátnymi príslušníkmi"[136].

Na používanie osobných údajov orgánmi konajúcimi na verejnej scéne sa vzťahuje aj článok 8 EDĽP.

Legitímne záujmy, ktoré plní prevádzkovateľ alebo tretia strana

Legitímne záujmy má nielen dotknutá osoba. V článku 7 písm. f) smernice o ochrane údajov sa stanovuje, že osobné údaje sa spracúvajú zákonne vtedy, keď je to „nevyhnutné pre účely legitímnych záujmov, ktoré plní kontrolór, alebo tretia strana alebo strany, ktorým sú údaje odhalené, s výnimkou, ak takéto záujmy sú prevýšené záujmami týkajúcimi sa základných práv a slobôd osoby pracujúcej s údajmi, ktoré potrebujú ochranu [...]".

V nasledujúcom rozsudku Súdny dvor rozhodol výslovne o článku 7 písm. f) smernice:

Príklad: SDEÚ vo veci *ASNEF a FECEMD*[137] 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 spracovanie údajov. Týkalo sa to situácie, keď španielsky právny predpis o ochrane údajov obsahoval ustanovenie, podľa ktorého by si iné súkromné strany mohli nárokovať legitímny záujem na spracovaní osobných údajov len vtedy, keď informácie predtým figurovali vo verejne prístupných zdrojoch.

136 Tamtiež, body 78 a 81.

137 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.

Súd najprv uviedol, že účelom smernice 95/46 je zaistiť rovnocennosť úrovne ochrany práv a slobôd jednotlivcov v súvislosti so spracovaním 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 v EÚ[138]. Následne SDEÚ konštatoval, že „z cieľa spočívajúceho v zabezpečení rovnakej úrovne ochrany vo všetkých členských štátoch vyplýva, že článok 7 smernice 95/46 stanovuje taxatívny zoznam prípadov, v ktorých možno spracovanie osobných údajov považovať za prípustné". Okrem toho „členské štáty nemôžu ani pridať nové zásady týkajúce sa zákonnosti spracovania osobných údajov do článku 7 smernice 95/46, ani stanoviť dodatočné požiadavky, ktoré by menili rozsah jednej zo šiestich zásad stanovených v tomto článku"[139]. Súdny dvor pripustil, že, „pokiaľ ide o zváženie potrebné podľa článku 7 písm. f) smernice 95/46, je možné zohľadniť, že závažnosť porušenia základných práv osoby dotknutej týmto spracovaním sa môže odlišovať v závislosti od toho, či predmetné údaje už figurujú, alebo ešte nefigurujú vo verejne prístupných zdrojoch".

Avšak „článok 7 písm. f) tejto smernice 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 Súdny dvor dospel k záveru, že „článok 7 písm. f) smernice 95/46 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"[140].

138 Tamtiež, bod 28. Pozri tiež smernicu o ochrane údajov, odôvodnenia 8 a 10.

139 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, body 30 a 32.

140 Tamtiež, body 40, 44, 48 a 49.

Podobné formulácie možno nájsť v odporúčaniach Rady Európy. Odporúčanie o profilovaní uznáva spracovanie osobných údajov na účely profilovania ako legitímne, ak je nevyhnutne potrebné z hľadiska legitímnych záujmov iných „okrem prípadov, keď sú takéto záujmy prevýšené základnými právami a slobodami dotknutých osôb“[141].

4.1.2. Zákonné spracúvanie citlivých údajov

V právnych predpisoch Rady Európy sa stanovenie primeranej ochrany pri používaní citlivých údajov ponecháva na vnútroštátnych právnych predpisoch, zatiaľ čo v **právnych predpisoch EÚ** v článku 8 smernice o ochrane údajov sa uvádza podrobný režim pre spracúvanie kategórií údajov, ktoré zverejňujú: rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie, členstvo v odboroch alebo informácie o zdravotnom stave a pohlavnom živote. Spracúvanie citlivých údajov je v zásade zakázané[142]. Existuje však podrobný zoznam výnimiek z tohto zákazu, ktoré sú vymenované v článku 8 ods. 2 a 3 smernice. Uvedené výnimky zahŕňajú výslovný súhlas dotknutej osoby, životné záujmy dotknutej osoby, legitímne záujmy iných a verejný záujem.

Na rozdiel od spracúvania údajov, ktoré nie sú citlivé, sa zmluvný vzťah s dotknutou osobou nepokladá za všeobecný základ legitímneho spracúvania citlivých údajov. Ak sa teda majú spracovať citlivé údaje v kontexte zmluvy s dotknutou osobou, použitie týchto údajov vyžaduje okrem súhlasu dotknutej osoby s uzatvorením zmluvného vzťahu aj jej samostatný výslovný súhlas so spracovaním údajov. Rovnakú hodnotu ako výslovný súhlas by však mala mať aj výslovná žiadosť dotknutej osoby o tovar alebo služby, ktorá nevyhnutne povedie ku zverejneniu citlivých údajov.

Príklad: Ak cestujúci leteckej spoločnosti požaduje v súvislosti s rezerváciou letenky, aby mu spoločnosť poskytla invalidný vozík alebo kóšer stravu, letecká spoločnosť smie tieto údaje použiť dokonca aj vtedy, ak cestujúci nepodpíše dodatočnú doložku o súhlase, v ktorej by sa uvádzalo, že cestujúci súhlasí s použitím svojich údajov zverejňujúcich informácie o jeho zdraví alebo náboženskom presvedčení.

141 Odporúčanie o profilovaní, článok 3.4 písm. b).

142 Smernica o ochrane údajov, článok 8 ods. 1.

Výslovný súhlas dotknutej osoby

Prvou podmienkou zákonného spracúvania akýchkoľvek údajov bez ohľadu na to, či sú alebo nie sú citlivé, je súhlas dotknutej osoby. V prípade citlivých údajov musí byť tento súhlas výslovný. Vo vnútroštátnych právnych predpisoch sa však môže stanoviť, že súhlas s používaním citlivých údajov nestačí ako právny základ povoľujúci ich spracúvanie[143], napríklad vo výnimočných prípadoch, keď spracúvanie znamená nezvyčajné riziko pre dotknutú osobu.

V jedinom osobitnom prípade sa za právny základ spracúvania citlivých údajov uznáva dokonca nevyslovený súhlas: v článku 8 ods. 2 písm. e) smernice sa stanovuje, že spracúvanie nie je zakázané, ak sa týka údajov, ktoré dotknutá osoba evidentne zverejnila. V tomto ustanovení sa zjavne predpokladá, že krok dotknutej osoby, ktorá svoje údaje zverejní, treba vykladať ako nevyslovený súhlas dotknutej osoby s použitím takýchto údajov.

Životné záujmy dotknutých osôb

Podobne ako pri údajoch, ktoré nie sú citlivé, možno aj citlivé údaje spracúvať z dôvodu životných záujmov dotknutej osoby[144].

V záujme legitímnosti spracúvania citlivých údajov na tomto základe platí nevyhnutná podmienka, že nie je možné požiadať dotknutú osobu o prijatie rozhodnutia, napríklad preto, lebo sa nachádza v bezvedomí alebo nie je prítomná a nedá sa zastihnúť.

Legitímne záujmy iných

Podobne ako pri údajoch, ktoré nie sú citlivé, môžu legitímne záujmy iných slúžiť ako základ spracúvania citlivých údajov. V prípade citlivých údajov a podľa článku 8 ods. 2 smernice o ochrane údajov sa to týka len nasledujúcich prípadov:

- ak je spracúvanie nevyhnutné z dôvodu životných záujmov inej osoby[145] a dotknutá osoba nie je fyzicky alebo právne spôsobilá poskytnúť svoj súhlas;

143 Tamtiež, článok 8 ods. 2 písm. a).

144 Tamtiež, článok 8 ods. 2 písm. c).

145 Tamtiež.

- ak sú citlivé údaje relevantné v oblasti pracovného práva, napríklad údaje týkajúce sa zdravia v súvislosti s osobitne nebezpečným pracoviskom, príp. údaje o náboženskom presvedčení v súvislosti so sviatkami[146];

- ak nadácie, združenia alebo iné neziskové organizácie s politickým, filozofickým, náboženským alebo odborárskym zameraním spracúvajú údaje o svojich členoch alebo sponzoroch alebo iných zúčastnených stranách (takéto údaje sú citlivé preto, pretože by pravdepodobne odhalili náboženské alebo politické presvedčenie príslušných jednotlivcov)[147];

- ak sa citlivé údaje používajú v kontexte súdnych alebo správnych konaní na ustanovenie, výkon alebo obranu právnych nárokov[148].

Okrem toho, podľa článku 8 ods. 3 smernice o ochrane údajov, ak sa údaje týkajúce sa zdravia používajú na účely lekárskeho vyšetrenia a liečby zo strany poskytovateľov zdravotnej starostlivosti, táto výnimka sa vzťahuje na spravovanie uvedených služieb. Osobitnú záruku predstavuje skutočnosť, že osoby sa považujú za „poskytovateľov zdravotnej starostlivosti" len vtedy, ak sa ich týkajú osobitné profesijné povinnosti zachovávania dôvernosti.

Verejný záujem

Ďalej podľa článku 8 ods. 4 smernice o ochrane údajov členské štáty môžu zaviesť ďalšie účely spracúvania citlivých údajov, a to v prípade, keď:

- dôvodom spracovania údajov je podstatný verejný záujem;

- je to stanovené vnútroštátnymi právnymi predpismi alebo rozhodnutím dozorného orgánu;

- vnútroštátne právne predpisy alebo rozhodnutie dozorného orgánu obsahujú nevyhnutné záruky s cieľom účinne chrániť záujmy dotknutých osôb[149].

Názorným príkladom sú systémy elektronickej zdravotnej dokumentácie, ktoré sa majú zriadiť v mnohých členských štátoch. Tieto systémy umožňujú sprístupnenie

146 Tamtiež, článok 8 ods. 2 písm. b).

147 Tamtiež, článok 8 ods. 2 písm. d).

148 Tamtiež, článok 8 ods. 2 písm. e).

149 *Tamtiež*, článok 8 ods. 4.

údajov týkajúcich sa zdravia, ktoré zozbierali poskytovatelia zdravotnej starostlivosti pri liečení pacienta, ďalším poskytovateľom zdravotnej starostlivosti danému pacientovi v rozsiahlom, zvyčajne celoštátnom meradle.

Pracovná skupina zriadená podľa článku 29 dospela k záveru, že zriadenie takýchto systémov by sa nemohlo uskutočniť v rámci platných právnych predpisov o spracúvaní údajov o pacientoch, založených na článku 8 ods. 3 smernice o ochrane údajov. Za predpokladu, že existencia systémov elektronickej zdravotnej dokumentácie predstavuje podstatný verejný záujem, možno vychádzať z článku 8 ods. 4 smernice, v ktorom sa vyžaduje výslovný právny základ pre ich zriadenie, ktorý takisto obsahuje nevyhnutné záruky na zaistenie bezpečného prevádzkovania systému[150].

4.2. Pravidlá bezpečnosti spracúvania

Hlavné body

- Z pravidiel bezpečnosti spracúvania vyplýva povinnosť prevádzkovateľa a sprostredkovateľa prijať primerané technické a organizačné opatrenia s cieľom zabrániť neoprávnenému zásahu do operácií spracovania údajov.
- Nevyhnutná úroveň bezpečnosti osobných údajov je, určená:
  - funkciami zabezpečenia dostupnými na trhu pre konkrétny typ spracúvania;
  - nákladmi;
  - citlivosťou spracúvaných údajov.
- Bezpečné spracúvanie osobných údajov je ďalej zaručené všeobecnou povinnosťou všetkých osôb, prevádzkovateľov alebo sprostredkovateľov zaistiť zachovanie dôvernosti údajov.

Povinnosť prevádzkovateľov a sprostredkovateľov prijať primerané opatrenia na zaistenie bezpečnosti osobných údajov je teda zakotvená v **právnych predpisoch Rady Európy o ochrane údajov,** ako aj **v právnych predpisoch EÚ o ochrane údajov**.

150 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.

4.2.1. Prvky bezpečnosti údajov

Podľa príslušných ustanovení **právnych predpisov EÚ**:

> *„Členské štáty zabezpečia, zavedenie príslušných technických a organizačných opatrení na ochranu osobných údajov pred náhodným alebo nezákonným poškodením alebo náhodnej strate, zmene, neoprávnenému prezradeniu alebo sprístupneniu, najmä, kde spracovanie obsahuje prenos údajov cez sieť a proti všetkým iným nezákonným formám spracovania. So zreteľom na stav techniky a cenu jej zavedenia takéto opatrenia zabezpečia úroveň bezpečnosti primeranú pre riziká, ktoré predstavuje spracovanie a charakter údajov, ktoré sa majú chrániť."*[151]

Podobné ustanovenie existuje v rámci **právnych predpisov Rady Európy**:

> *„Prijmú sa primerané bezpečnostné opatrenia na ochranu osobných údajov v automatizovaných súboroch údajov pred náhodným alebo nepovoleným zničením alebo pred náhodnou stratou, ako aj pred nepovoleným prístupom, zmenami alebo šírením."*[152]

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 – European Privacy Seal (EuroPriSe) v rámci európskeho programu podpory transeurópskych telekomunikačných sietí (eTEN), skúmajúci možnosti certifikácie produktov, predovšetkým softvéru, ktoré sú v súlade s európskymi právnymi predpismi 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 ne[153]. Agentúra ENISA pravidelne zverejňuje analýzy aktuálnych bezpečnostných hrozieb a radí, ako na ne reagovať.

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 nasledujúce okruhy:

151 Smernica o ochrane údajov, článok 17 ods. 1.

152 Dohovor č. 108, článok 7.

153 Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, Ú. v. EÚ L 77, 2004.

- pravidelné informovanie všetkých zamestnancov o pravidlách bezpečnosti osobných údajov a ich povinnostiach vyplývajúcich z právnych predpisov o ochrane údajov, predovšetkým pokiaľ ide o povinnosti týkajúce sa dôvernosti;

- 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 na miesta a k hardvéru a softvéru prevádzkovateľa alebo sprostredkovateľa vrátane kontrol povolenia na prístup;

- zaistenie toho, aby povolenia na prístup k osobným údajom udeľovala oprávnená osoba a aby bolo potrebné predloženie príslušných dokladov;

- automatizácia protokolov prístupu k osobným údajom elektronickými prostriedkami a pravidelné kontroly takýchto protokolov interným dozorným oddelením;

- dôkladné zdokumentovanie iných foriem zverejnenia než je automatizovaný prístup k údajom s cieľom môcť preukázať, že nedošlo k žiadnemu nezákonnému prenosu údajov.

Dôležitou súčasťou efektívnych 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 vhodné opatrenia boli nielen napísané, 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 úradníci na ochranu údajov, bezpečnostné vzdelávanie zamestnancov, pravidelné audity, penetračné testovanie a pečate kvality.

Príklad: Sťažovateľka vo veci *I./Fínsko*[154] nebola schopná dokázať, že jej zdravotné záznamy boli nezákonne sprístupnené ďalším zamestnancom nemocnice, v ktorej

154 ESĽP, *I./Fínsko*, č. 20511/03, 17. Júla 2008.

pracovala. Vnútroštátne súdy preto zamietli jej sťažnosť na porušenie práva na ochranu údajov. ESĽP dospel k záveru, že došlo k porušeniu článku 8 EDĽP, 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 ostatných nahliadnutí a tieto informácie boli odstránené po vrátení spisu do archívu". Pre súd bolo rozhodujúce, že systém zriadený v nemocnici zjavne nebol v súlade s právnymi požiadavkami obsiahnutými v domácich právnych predpisoch a vnútroštátne súdy túto skutočnosť náležite nezohľadnili.

Oznámenia o porušení ochrany údajov

Niekoľko európskych krajín zaviedlo v rámci právnych predpisov o ochrane osobných údajov nový nástroj na riešenie porušenia bezpečnosti osobných údajov: povinnosť poskytovateľov elektronických komunikačných služieb oznamovať prípady porušenia ochrany osobných údajov pravdepodobným obetiam a dozorným orgánom. Z právnych predpisov EÚ vyplýva, že zaslanie oznámenia o porušení ochrany údajov je pre poskytovateľov telekomunikačných služieb povinné[155]. Účelom oznámení o porušení ochrany údajov dotknutým osobám je predísť škodám: oznámenie o porušení ochrany osobných údajov a možných dôsledkoch minimalizuje riziko negatívneho vplyvu na dotknuté osoby. V prípadoch závažnej nedbalosti je takisto možné udeliť poskytovateľom pokutu.

Je nutné, aby vnútorné postupy na účinné riadenie a oznamovanie porušení ochrany osobných údajov boli stanovené vopred, keďže časový rámec povinnosti oznámiť porušenie dotknutým osobám a/alebo dozorným orgánom, stanovený vnútroštátnymi právnymi predpismi, je pomerne krátky.

4.2.2. Dôvernosť

V právnych predpisoch EÚ je bezpečné spracovanie osobných údajov je ďalej zaručené všeobecnou povinnosťou všetkých osôb, prevádzkovateľov alebo sprostredkovateľov, zaistiť dôvernosť údajov.

155 Pozri smernicu 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, článok 4 ods. 3, zmenenú 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; pozri tiež smernicu 2002/58/ES týkajúcu 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.

Príklad: Zamestnankyňa poisťovacej spoločnosti telefonuje na pracovisku s osobou, ktorá tvrdí, že je klientom poisťovne a požaduje informácie týkajúce sa príslušnej poistnej 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.

V článku 16 smernice o ochrane údajov sa dôvernosť uvádza len v rámci vzťahu prevádzkovateľ – sprostredkovateľ. Otázkou záväznosti zachovania dôvernosti údajov pre prevádzkovateľov v tom zmysle, či smú údaje zverejniť tretím stranám, sa zaoberá v článkoch 7 a 8 smernice.

Povinnosť dôvernosti sa netýka situácií, keď sa osoba údaje nedozvedela ako zamestnanec prevádzkovateľa alebo sprostredkovateľa, ale sama ako súkromný jednotlivec. V tomto prípade sa neuplatňuje článok 16 smernice o ochrane údajov, keďže použitie osobných údajov súkromnými jednotlivcami je úplne vyňaté z rozsahu pôsobnosti smernice a patrí do rámca tzv. výnimky pre domácnosti[156]. Výnimkou pre domácnosti sa rozumie používanie osobných údajov „fyzickou osobou v priebehu osobnej činnosti, alebo činnosti týkajúcej sa domácnosti“[157]. Podľa rozhodnutia SDEÚ vo veci *Bodil Lindqvist*[158] sa však táto výnimka musí interpretovať v užšom zmysle, najmä pokiaľ ide o zverejňovanie údajov. Konkrétne sa výnimka pre domácnosti netýka sprístupnenia osobných údajov neobmedzenému počtu príjemcov na internete (podrobnejšie informácie o tejto veci nájdete v oddieloch 2.1.2, 2.2, 2.3.1 a 6.1).

V právnych predpisoch Rady Európy vyplýva povinnosť dôvernosti z pojmu bezpečnosti osobných údajov v článku 7 dohovoru č. 108, ktorý je venovaný bezpečnosti osobných údajov.

Z hľadiska sprostredkovateľov dôvernosť znamená, že osobné údaje, ktoré im zveril prevádzkovateľ, môžu používať len v súlade s pokynmi prevádzkovateľa. Z hľadiska zamestnancov prevádzkovateľa alebo sprostredkovateľa si dôvernosť vyžaduje, aby osobné údaje používali len podľa pokynov príslušných nadriadených.

156 Smernica o ochrane údajov, článok 3 ods. 2 druhá zarážka.

157 Tamtiež.

158 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003.

Povinnosť dôvernosti 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 dôvernosti, bežne zaručenú zahrnutím doložiek o dôvernosti do pracovnej zmluvy zamestnanca.

Porušenie profesijnej povinnosti dôvernosti je postihnuteľné v rámci trestného práva vo viacerých členských štátoch EÚ a zmluvných stranách dohovoru č. 108.

4.3. Pravidlá transparentnosti spracúvania

Hlavné body

- Prevádzkovateľ musí pred začiatkom spracovania osobných údajov minimálne informovať dotknuté osoby o totožnosti prevádzkovateľa a účele spracúvania údajov, okrem prípadov, keď dotknutá osoba už má tieto údaje k dispozícii.
- V prípade, že sa údaje zbierajú od tretích strán, povinnosť poskytovať informácie sa neuplatňuje, ak:
  - je spracúvanie údajov stanovené zákonom alebo
  - sa ukáže, že poskytnutie informácií je nemožné, prípadne by si vyžadovalo neprimerané úsilie.
- Pred začiatkom spracovania osobných údajov prevádzkovateľ okrem toho musí:
  - oznámiť orgánu dozoru zamýšľané operácie spracúvania alebo
  - nechať spracúvanie interne zdokumentovať nezávislým úradníkom na ochranu údajov, ak sa takýto postup stanovuje vo vnútroštátnych právnych predpisoch.

Zásada prijateľného spracúvania si vyžaduje transparentnosť spracúvania. **V právnych predpisoch Rady Európy** sa v tejto súvislosti stanovuje, že každá osoba musí mať možnosť dozvedieť sa o existencii súborov údajov, ktoré sa spracúvajú, ich účele a príslušnom prevádzkovateľovi[159]. Spôsob splnenia tejto požiadavky sa ponecháva na vnútroštátnych právnych predpisoch. **Právne predpisy EÚ** sú konkrétnejšie a zaručuje sa v nich transparentnosť pre dotknutú osobu prostredníctvom povinnosti prevádzkovateľa informovať dotknutú osobu a širokú verejnosť formou oznámenia.

159 Dohovor č. 108, článok 8 písm. a).

V oboch právnych systémoch môžu existovať výnimky a obmedzenia súvisiace s povinnosťou transparentnosti prevádzkovateľa, ak takéto obmedzenie predstavuje opatrenie nevyhnutne potrebné na zabezpečenie určitých verejných záujmov alebo ochranu dotknutých osôb alebo práv a slobôd iných, pokiaľ je to nevyhnutné v demokratickej spoločnosti[160]. Výnimky môžu byť napríklad nutné v súvislosti s vyšetrovaním trestného činu, ale môžu byť opodstatnené aj za iných okolností.

4.3.1. Informácie

Podľa právnych predpisov Rady Európy, ako aj podľa právnych predpisov EÚ, sú prevádzkovatelia operácií spracúvania povinní vopred informovať dotknuté osoby o zamýšľanom spracúvaní[161]. Táto požiadavka nezávisí od žiadosti dotknutej osoby, ale o jej splnenie musí aktívne usilovať prevádzkovateľ, a to bez ohľadu na to, či dotknutá osoba prejavuje záujem o informácie alebo nie.

Obsah informácií

Informácie musia zahŕňať účel spracúvania, ako aj totožnosť a kontaktné údaje prevádzkovateľa[162]. V smernici o ochrane údajov sa vyžaduje poskytnutie ďalších informácií, „pokiaľ sú takéto ďalšie informácie potrebné, so zreteľom na špecifické okolnosti za ktorých sa údaje zhromažďujú, zaručenie správneho spracovania vzhľadom na osobu pracujúcu s údajmi“. V článkoch 10 a 11 smernice sa okrem iného uvádzajú kategórie spracovaných údajov a príjemcovia takýchto údajov, ako aj existencia práva prístupu k údajom a práva na ich opravu. Keď sa zbierajú údaje od dotknutých osôb, v informáciách by sa malo ozrejmiť, či sú odpovede povinné alebo dobrovoľné, ako aj možné dôsledky neodoslania odpovede[163].

Z hľadiska právnych predpisov Rady Európy sa poskytovanie takýchto informácií môže považovať za osvedčený postup v rámci zásady prijateľného spracúvania údajov a v tomto zmysle aj za súčasť právnych predpisov Rady Európy.

Zásada prijateľného spracúvania si vyžaduje, aby dotknutá osoba dokázala informácie ľahko pochopiť. Musí sa použiť jazyk, ktorý je pre adresáta primeraný. Úroveň

160 Tamtiež, článok 9 ods. 2 a smernica o ochrane údajov, článok 13 ods. 1.

161 Dohovor č. 108, článok 8 písm. a) a smernica o ochrane údajov, článok 10 a 11.

162 Dohovor č. 108, článok 8 písm. a) a smernica o ochrane údajov, článok 10 písm. a) a b).

163 Smernica o ochrane údajov, článok 10 písm. c).

a druh použitého jazyka sa bude musieť líšiť podľa toho, či sú zamýšľaní adresáti napríklad dospelí alebo deti, široká verejnosť alebo vysokoškolskí odborníci.

Niektoré dotknuté osoby budú chcieť byť informované len stručne o tom, ako a prečo sa ich údaje spracúvajú, zatiaľ čo iné osoby budú vyžadovať podrobné vysvetlenie. Nad vyvážením týchto aspektov prijateľného informovania sa zamýšľa v stanovisku pracovnej skupiny zriadenej podľa článku 29, v ktorom sa presadzuje myšlienku tzv. viacúrovňových oznámení[164] umožňujúcich dotknutým osobám, aby sa rozhodli, ktorú úroveň podrobnosti uprednostnia.

Čas poskytovania informácií

Smernica o ochrane údajov obsahuje nepatrne odlišné ustanovenia týkajúce sa času, v ktorom je nutné poskytnúť informácie, a to podľa toho, či sú údaje zozbierané od dotknutej osoby (článok 10) alebo od tretej strany (článok 11). Ak sa údaje zbierajú od dotknutej osoby, informácie sa musia poskytnúť najneskôr v čase zberu. Ak sa údaje zbierajú od tretích strán, informácie sa musia poskytnúť buď najneskôr vo chvíli, keď prevádzkovateľ údaje zaznamená, alebo pred prvým zverejnením údajov tretej strane.

Výnimky z povinnosti informovať

V rámci právnych predpisov EÚ, existuje všeobecná výnimka z povinnosti informovať dotknutú osobu v prípade, že dotknutá osoba už dané informácie má[165]. Týka sa to situácií, keď dotknutá osoba už bude (podľa okolností konkrétneho prípadu) vedieť o tom, že prevádzkovateľ spracuje jej údaje na určitý účel.

V článku 11 smernice, ktorý sa týka povinnosti informovať dotknutú osobu, ak údaje neboli získané od nej, sa takisto stanovuje, že povinnosť informovať nebude platiť v prípade spracúvania na štatistické účely alebo na účely historického či vedeckého výskumu, ak:

- sa poskytnutie takýchto informácií ukáže ako nemožné alebo
- by si vyžadovalo neprimerané úsilie, alebo

164 Pracovná skupina zriadená podľa článku 29 (2004), *stanovisko 10/2004 ku harmonizovanejším ustanoveniam o poskytovaní informácií*, WP 100, Brusel, 25. novembra 2004.

165 Smernica o ochrane údajov, článok 10 a článok 11 ods. 1.

- zaznamenanie alebo zverejnenie údajov je výslovne stanovené zákonom[166].

Len v článku 11 ods. 2 smernice o ochrane údajov sa uvádza, že dotknuté osoby nemusia byť informované o operáciách spracúvania, ak sú tieto operácie stanovené zákonom. Vzhľadom na všeobecný právny predpoklad, že právne predpisy sú známe subjektom, ktorých sa týkajú, je možné namietať, že ak sa údaje zbierajú od dotknutej osoby podľa článku 10 smernice, dotknutá osoba je informovaná. Vzhľadom na to, že znalosť právnych predpisov je len predpoklad, zásada prijateľného spracúvania by si podľa článku 10 vyžadovala, aby dotknuté osoby boli informované dokonca aj vtedy, keď je spracúvanie stanovené zákonom, predovšetkým preto, lebo informovanie dotknutej osoby nie je mimoriadne náročné, pokiaľ sa údaje zbierajú priamo od nej. **V rámci právnych predpisov Rady Európy** sa v dohovore č. 108 sa výslovne uvádzajú výnimky z článku 8. Výnimky stanovené v článkoch 10 a 11 smernice o ochrane údajov opäť možno chápať ako príklady osvedčeného postupu pre výnimky podľa článku 9 dohovoru č. 108.

Rôzne spôsoby poskytovania informácií

Ideálnym spôsobom poskytnutia informácií by bolo ústne alebo písomné oslovenie každej jednotlivej dotknutej osoby. Ak sa údaje zberajú od dotknutej osoby, poskytnutie informácií by sa malo spojiť so zberom údajov. Predovšetkým vtedy, keď sa údaje zberajú od tretích strán, a vzhľadom na zrejmé praktické ťažkosti pri osobnom oslovovaní dotknutých osôb, je možné poskytnúť informácie formou vhodného oznámenia.

Jedným z najúčinnejších spôsobov poskytnutia informácií bude uvedenie vhodných informačných doložiek na domovskej stránke prevádzkovateľa, napríklad doložky o zásadách ochrany osobných údajov na webovej lokalite. V zásadách spoločnosti alebo verejného orgánu týkajúcich sa informácií sa musí zohľadniť skutočnosť, že existuje veľká časť obyvateľov, ktorá nepoužíva internet.

4.3.2. Oznámenie

Vo vnútroštátnych právnych predpisoch sa prevádzkovateľom môže ukladať povinnosť informovať príslušný dozorný orgán o operáciách spracúvania, aby mohli byť uverejnené. Vo vnútroštátnych právnych predpisoch sa môže takisto stanoviť, že prevádzkovatelia môžu zamestnávať zodpovednú osobu, ktorá zodpovedá za

166 Tamtiež, odôvodenie 40 a článok 11 ods. 2.

vedenie registra operácií spracúvania vykonávaných prevádzkovateľom[167]. Tento interný register musí byť verejnosti sprístupnený na požiadanie.

Príklad: V oznámení, ako aj v dokumentácii internej zodpovednej osoby, sa musia opisovať hlavné vlastnosti predmetného spracúvania údajov. Bude obsahovať informácie o prevádzkovateľovi, účele spracúvania, právnom základe spracúvania, kategóriách spracúvaných údajov, pravdepodobných príjemcoch tretích strán, ako aj informácie o tom, či sa zamýšľajú alebo nezamýšľajú cezhraničné toky údajov a ak áno, o ktoré toky pôjde.

Uverejnenie oznámení dozorným orgánom musí mať podobu osobitného registra. Aby register splnil stanovený cieľ, musí umožňovať jednoduchý a bezplatný prístup. To sa týka aj dokumentácie vedenej zodpovednou osobou pôsobiacou u prevádzkovateľa.

Výnimky z povinnosti zasielať oznámenia príslušnému dozornému orgánu alebo zamestnávať internú zodpovednú osobu môžu byť stanovené vnútroštátnymi právnymi predpismi pre operácie spracúvania, ktoré pravdepodobne nebudú znamenať žiadne konkrétne riziko pre dotknuté osoby, sú uvedené v článku 18 ods. 2 smernice o ochrane údajov[168].

4.4. Pravidlá podpory súladu

Hlavné body

- V smernici o ochrane údajov sa rozvíja zásada zodpovednosti a v tejto súvislosti sa tu uvádza niekoľko nástrojov na podporu súladu:
  - predbežná kontrola zamýšľaných operácií spracúvania vnútroštátnym dozorným orgánom;
  - zodpovedné osoby, ktoré poskytnú prevádzkovateľovi osobitné odborné znalosti v oblasti ochrany údajov;
  - kódexy správania spresňujúce existujúce pravidlá ochrany údajov na uplatnenie v odvetví spoločnosti, najmä v podnikaní.

167 Tamtiež, článok 18 ods. 2 druhá zarážka.

168 Tamtiež, článok 18 ods. 2 prvá zarážka.

- V právnych predpisoch Rady Európy sa navrhujú podobné nástroje na podporu súladu v odporúčaní o profilovaní.

4.4.1. Predbežná kontrola

Podľa článku 20 smernice o ochrane údajov musí dozorný orgán pred začiatkom spracúvania skontrolovať operácie spracúvania, ktoré by mohli predstavovať špecifické riziká pre práva a slobody dotknutých osôb z dôvodu účelu alebo okolností spracúvania. Operácie spracúvania, pri ktorých sa musí vykonať predbežná kontrola, sú určené vo vnútroštátnych právnych predpisoch. Výsledkom predbežnej kontroly môže byť zákaz operácií spracúvania alebo zmena vlastností v navrhovanom spôsobe vykonania týchto operácií. Cieľom článku 20 smernice je zaistiť, aby sa zbytočne rizikové spracúvanie ani nezačalo, keďže dozorný orgán je oprávnený zakázať takéto operácie. Podmienkou účinnosti tohto mechanizmu je informovanosť dozorného orgánu. Dozorný orgán bude potrebovať donucovacie právomoci, napríklad možnosť pokutovať prevádzkovateľov, aby zabezpečil plnenie oznamovacej povinnosti z ich strany.

Príklad: Ak spoločnosť vykonáva operácie spracúvania, na ktoré sa podľa vnútroštátnych právnych predpisov vzťahuje predbežná kontrola, musí predložiť dokumentáciu o plánovaných operáciách spracúvania dozornému orgánu. Spoločnosť nesmie začať operácie spracúvania skôr, ako dostane od dozorného orgánu kladnú odpoveď.

V niektorých členských štátoch sa vo vnútroštátnych právnych predpisoch alternatívne stanovuje, že operácie spracúvania sa smú začať vtedy, keď dozorný orgán v určitej lehote, napríklad do troch mesiacov, nereaguje na zaslané oznámenie.

4.4.2. Zodpovedné osoby

Smernica o ochrane údajov obsahuje možnosť, aby sa vo vnútroštátnych právnych predpisoch stanovilo, že prevádzkovatelia môžu vymenovať úradníka do funkcie zodpovednej osoby[169]. Cieľom tejto funkcie je zaistiť, aby operácie spracúvania nepriaznivo neovplyvnili práva a slobody dotknutých osôb[170].

169 Tamtiež, článok 18 ods. 2 druhá zarážka.

170 Tamtiež.

Príklad: V nemeckom spolkovom zákone o ochrane údajov (*Bundesdatenschutzgesetz*) sa v oddiele 4f pododdiele 1 požaduje, aby spoločnosti v súkromnom vlastníctve vymenovali internú zodpovednú osobu, ak na účely automatizovaného spracúvania osobných údajov trvalo zamestnávajú 10 alebo viac osôb.

Dosiahnutie tohto cieľa si vyžaduje určitú mieru nezávislosti uvedenej zodpovednej osoby v rámci organizácie prevádzkovateľa, na čo sa výslovne poukazuje aj v smernici. Ďalšou podmienkou efektívneho fungovania tejto funkcie sú silné zamestnanecké práva na ochranu pred takými prípadmi, ako je napríklad neoprávnené prepustenie.

Pojem zodpovednej osoby sa zaviedol v záujme súladu s vnútroštátnymi právnymi predpismi o ochrane údajov aj v niektorých odporúčaniach Rady Európy[171].

4.4.3. Kódexy správania

Podniky a ďalšie odvetvia môžu v záujme podpory súladu vypracovať podrobné pravidlá, ktorými upravia svoje obvyklé činnosti pri spracúvaní údajov a kodifikujú najlepšie postupy. Expertíza členov odvetvia pomôže nachádzať praktické riešenia, ktoré sa pravdepodobne uplatnia. Podobne sa nabádajú členské štáty, ako aj Európska komisia, aby podporovali vypracovanie kódexov správania, ktoré majú prispieť k správnemu vykonávaniu vnútroštátnych ustanovení prijatých členskými štátmi v súlade so smernicou, pričom sa zohľadnia osobitné vlastnosti rôznych odvetví[172].

Členské štáty musia v záujme zaistenia súladu kódexov správania s vnútroštátnymi ustanoveniami prijatými na základe smernice o ochrane údajov vypracovať postup hodnotenia kódexov. V tomto postupe by sa spravidla vyžadovalo zapojenie vnútroštátneho orgánu, odborových zväzov a ďalších orgánov zastupujúcich ostatné kategórie prevádzkovateľov[173].

Návrhy kódexov Spoločenstva a zmeny alebo rozšírenie platných kódexov Spoločenstva je možné predkladať na hodnotenie pracovnej skupine zriadenej podľa článku 29. Po schválení pracovnou skupinou môže Európska komisia zaistiť primeranú publicitu kódexov[174].

171 Pozri napríklad Odporúčanie o profilovaní, článok 8.3.

172 Smernica o ochrane údajov, článok 27 ods. 1.

173 Tamtiež, článok 27 ods. 2.

174 Tamtiež, článok 27 ods. 3.

Príklad: Európska federácia priameho a interaktívneho marketingu (FEDMA) vypracovala Európsky kódex postupu pri používaní údajov v rámci priameho marketingu. Kódex bol úspešne predložený pracovnej skupine zriadenej podľa článku 29. V roku 2010 bola do kódexu doplnená príloha týkajúca sa elektronickej marketingovej komunikácie[175].

175 Pracovná skupina zriadená podľa článku 29 (2010), *stanovisko 4/2010 k Európskemu kódexu správania Európskej federácie priameho marketingu (FEDMA) pre používanie osobných údajov v priamom marketingu*, WP 174, 13. júla 2010.

5

Práva dotknutých subjektov a ich presadzovanie

EÚ	Zahrnuté otázky	Rada Európy
Právo prístupu		
Smernica o ochrane údajov, článok 12 SDEÚ, C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 7. mája 2009	**Právo prístupu k vlastným údajom**	Dohovor č. 108, článok 8 písm. b)
	Právo úpravy, vymazania (výmaz) alebo zablokovania	Dohovor č. 108, článok 8 písm. c) ESĽP, *Cemalettin Canli/Turecko*, č. 22427/04, 18. novembra 2008 ESĽP, *Segerstedt-Wiberg a iní/Švédsko*, č. 62332/00, 6. júna 2006 ESĽP, *Ciubotaru/Moldavsko*, č. 27138/04, 27. apríla 2010
Právo námietky		
Smernica o ochrane údajov, článok 14 ods. 1 písm. a)	**Právo námietky z dôvodu konkrétnej situácie dotknutej osoby**	Odporúčanie o profilovaní, článok 5.3
Smernica o ochrane údajov, článok 14 ods. 1 písm. b)	**Právo námietky proti ďalšiemu použitiu údajov na marketingové účely**	Odporúčanie o priamom marketingu, článok 4.1
Smernica o ochrane údajov, článok 15	**Právo námietky proti automatizovaným rozhodnutiam**	Odporúčanie o profilovaní, článok 5.5

EÚ	Zahrnuté otázky	Rada Európy
Nezávislý dohľad		
Charta, článok 8 ods. 3 Smernica o ochrane údajov, článok 28 Nariadenie o ochrane údajov inštitúciami EÚ, kapitola V Nariadenie o ochrane údajov SDEÚ, C-518/07, *Európska komisia/Spolková republika Nemecko*, 9. marca 2010 SDEÚ, C-614/10, *Európska komisia/Rakúska republika*, 16. októbra 2012 SDEÚ, C-288/12, *Európska komisia/Maďarsko*, 8. apríla 2014	**Vnútroštátne dozorné orgány**	Dohovor č. 108, dodatkový protokol, článok 1
Prostriedky nápravy a sankcie		
Smernica o ochrane údajov, článok 12	**Žiadosť adresovaná prevádzkovateľovi**	Dohovor č. 108, článok 8 písm. b)
Smernica o ochrane údajov, článok 28 ods. 4 Nariadenie o ochrane údajov inštitúciami EÚ, článok 32 ods. 2	**Sťažnosti predložené dozornému orgánu**	Dohovor č. 108, dodatkový protokol, článok 1 ods. 2 písm. b)
Charta, článok 47	**Súdy (vo všeobecnosti)**	EDĽP, článok 13
Smernica o ochrane údajov, článok 28 ods. 3	**Vnútroštátne súdy**	Dohovor č. 108, dodatkový protokol, článok 1 ods. 4
ZFEÚ, článok 263 ods. 4 Nariadenie o ochrane údajov inštitúciami EÚ, článok 32 ods. 1 ZFEÚ, článok 267	**SDEÚ**	
	ESĽP	EDĽP, článok 34
Prostriedky nápravy a sankcie		
Charta, článok 47 Smernica o ochrane údajov, článok 22 a 23 SDEÚ, C-14/83, *Sabine von Colson a Elisabeth Kamann/Land Nordrhein-Westfalen*, 10. apríla 1984 SDEÚ, C-152/84, *M. H. Marshall/Southampton and South-West Hampshire Area Health Authority*, 26. februára 1986	**Za porušenie vnútroštátnych predpisov o ochrane údajov**	EDĽP, článok 13 (len pre členské štáty RE) Dohovor č. 108, článok 10 ESĽP, *K.U./Fínsko*, č. 2872/02, 2. marca 2008 EDĽP, *Biriuk/Litva*, č. 23373/03, 25. novembra 2008
Nariadenie o ochrane údajov inštitúciami EÚ, články 34 a 49 SDEÚ, C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd*, 29. júna 2010	**Za porušenie právnych predpisov EÚ inštitúciami a orgánmi EÚ**	

Účinnosť právnych predpisov vo všeobecnosti a konkrétne práv dotknutých osôb závisí do značnej miery od existencie vhodných mechanizmov na ich presadzovanie. V rámci európskych právnych predpisov o ochrane údajov musia vnútroštátne právne predpisy oprávňovať dotknutú osobu, aby chránila svoje údaje. Vo vnútroštátnych právnych predpisoch sa musí takisto stanovovať zriadenie nezávislých dozorných orgánov, ktoré majú dotknutým osobám pomáhať pri vykonávaní ich práv a dozerať na spracúvanie osobných údajov. Okrem toho z práva na účinný prostriedok nápravy zaručeného podľa EDĽP a charty vyplýva požiadavka, aby prostriedky nápravy boli dostupné každej osobe.

5.1. Práva dotknutých osôb

Hlavné body

- Každý má podľa vnútroštátnych právnych predpisov právo vyžiadať si od akéhokoľvek prevádzkovateľa informácie o tom, či spracúva alebo nespracúva jeho údaje.
- Dotknuté osoby majú podľa vnútroštátnych právnych predpisov:
  - právo prístupu ku svojim údajom u každého prevádzkovateľa, ktorý takéto údaje spracúva;
  - právo úpravy údajov (alebo podľa okolností zablokovania) prevádzkovateľom spracúvajúcim ich údaje v prípade, že sú tieto údaje nepresné;
  - právo vymazania alebo zablokovania údajov (podľa okolností) prevádzkovateľom, ak ich údaje spracúva nezákonne.
- Dotknuté osoby majú okrem toho právo námietky u prevádzkovateľa proti:
  - automatizovaným rozhodnutiam (prijatým s použitím osobných údajov spracúvaných výlučne automatickými prostriedkami);
  - spracúvaniu ich údajov, ak takéto spracúvanie vedie k nevyváženým výsledkom;
  - použitiu ich údajov na priame marketingové účely.

5.1.1. Právo prístupu

V rámci právnych predpisov EÚ sú v článku 12 smernice o ochrane údajov uvedené zložky práva prístupu dotknutej osoby vrátane práva získať „potvrdenie týkajúce sa toho, či sa spracovávajú (alebo nie) údaje, ktoré sa [jej] týkajú a informácie aspoň

podľa účelov spracovania, kategórií uvedených údajov a príjemcov alebo kategórií príjemcov, ktorým sa údaje oznámili“, ako aj práva na „úpravu, vymazanie alebo zablokovanie údajov, ktorých spracovanie nezodpovedá ustanoveniam tejto smernice, najmä z dôvodu neúplného alebo nepresného charakteru údajov“.

V rámci právnych predpisov Rady Európy existujú rovnaké práva, ktoré musia byť zakotvené vo vnútroštátnych právnych predpisoch (článok 8 dohovoru č. 108). V niekoľkých odporúčaniach Rady Európy je použitý termín „prístup“, opisujú sa v nich rôzne aspekty práva prístupu a navrhuje sa ich zavádzanie do vnútroštátnych právnych predpisoch rovnakým spôsobom, aký je opísaný v predchádzajúcom odseku.

Podľa článku 9 dohovoru č. 108 a článku 13 smernice o ochrane údajov je možné povinnosť prevádzkovateľa reagovať na žiadosť dotknutej osoby o prístup obmedziť z dôvodu prednostných právnych záujmov iných. Prednostné právne záujmy môžu zahŕňať verejné záujmy, napríklad vnútroštátnu bezpečnosť, verejnú bezpečnosť a stíhanie trestných činov, ako aj súkromné záujmy, ktoré sú naliehavejšie ako záujmy ochrany údajov. Prípadné výnimky alebo obmedzenia musia byť nevyhnutné v demokratickej spoločnosti a primerané stanovenému cieľu. Vo výnimočných prípadoch, napríklad z dôvodu zdravotných indikácií, si môže ochrana dotknutej osoby ako taká vyžadovať obmedzenie transparentnosti. Týka sa to predovšetkým obmedzenia práva prístupu každej dotknutej osoby.

Ak sa údaje spracúvajú výlučne na účely vedeckého výskumu alebo štatistické účely, smernicou o ochrane údajov sa povoľuje obmedzenie práv prístupu vnútroštátnymi právnymi predpismi, je však nutné stanoviť primerané právne záruky. Predovšetkým treba zaistiť, že sa v súvislosti s takýmto spracúvaním údajov neprijmú žiadne opatrenia ani rozhodnutia týkajúce sa konkrétneho jednotlivca a že „očividne nie je žiadne riziko porušenia súkromia osoby pracujúcej s údajmi“[176]. Podobné ustanovenia sú zahrnuté do článku 9 ods. 3 dohovoru č. 108.

Právo prístupu k vlastným údajom

Podľa právnych predpisov Rady Európy je právo prístupu k vlastným údajom výslovne uznané v článku 8 dohovoru č. 108. ESĽP opakovane potvrdil, že existuje právo prístupu k informáciám o osobných údajoch osoby, ktoré uchovávajú alebo

176 Smernica o ochrane údajov, článok 13 ods. 2.

používajú iní, a že toto právo vyplýva z potreby rešpektovať súkromný život[177]. ESĽP vo veci *Leander*[178] však dospel k záveru, že právo prístupu k osobným informáciám uchovávaným verejnými orgánmi môže byť za určitých okolností obmedzené.

Podľa právnych predpisov EÚ je právo prístupu k vlastným údajom výslovne uznané v článku 12 smernice o ochrane údajov a ako základné právo v článku 8 ods. 2 charty.

V článku 12 písm. a) smernice sa stanovuje, že členské štáty musia každej dotknutej osobe zaručiť právo prístupu k jej osobným údajom a informáciám. Každá dotknutá osoba má konkrétne právo na to, aby jej prevádzkovateľ potvrdil, či spracúva alebo nespracúva údaje, ktoré sa jej týkajú, ako aj na informácie zahŕňajúce aspoň nasledujúce oblasti:

- účely spracúvania;
- kategórie dotknutých údajov;
- údaje, ktoré sa spracúvajú;
- príjemcovia alebo kategórie príjemcov, ktorým sa údaje zverejňujú;
- všetky dostupné informácie o zdroji údajov, ktoré sa spracúvajú;
- v prípade automatizovaných rozhodnutí logika každého automatického spracúvania údajov.

Vo vnútroštátnych právnych predpisoch možno uviesť ďalšie informácie, ktoré musí prevádzkovateľ poskytnúť, napríklad musí uviesť právny základ oprávňujúci spracúvanie údajov.

Príklad: Osoba, ktorá získa prístup k osobným údajom, je schopná určiť, či sú tieto údaje presné alebo nie. Je preto nevyhnutne potrebné, aby dotknutá osoba bola informovaná o kategóriách spracovaných údajov, ako aj o ich obsahu.

177 ESĽP, *Gaskin/Spojené kráľovstvo*, č. 10454/83, 7. Júla 1989; ESĽP, *Odièvre/Francúzsko* [VK], č. 42326/98, 13. Februára 2003; ESĽP, *K.H. a iní/Slovensko*, č. 32881/04, 28. apríla 2009; ESĽP, *Godelli/Taliansko*, č. 33783/09, 25. septembra 2012.

178 ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987.

Nestačí, že prevádzkovateľ oznámi dotknutej osobe, že spracúva jej meno, adresu, dátum narodenia a oblasť záujmov. Musí jej oznámiť, že spracúva „meno: N. N.; adresu: 1040 Viedeň, Schwarzenbergplatz 11, Rakúsko; dátum narodenia: 10. 10. 1974; oblasť záujmov (podľa vyhlásenia dotknutej osoby): vážna hudba". Posledná položka obsahuje dodatočné informácie o zdroji údajov.

Oznámenie dotknutej osobe o spracúvaných údajoch a poskytnutie všetkých dostupných informácií o zdroji týchto údajov musia mať zrozumiteľnú formu, čo znamená, že prevádzkovateľ musí dotknutej osobe podrobnejšie vysvetliť, čo znamená spracovanie. Napríklad obvykle nestačí výlučné citovanie technických skratiek alebo lekárskych termínov v odpovedi na žiadosť o prístup, a to dokonca ani vtedy, ak sa uchovávajú len uvedené skratky či termíny.

Informácie o zdroji údajov, ktoré prevádzkovateľ spracúva, musia byť uvedené v odpovedi na žiadosť o prístup v takom rozsahu, v akom sú k dispozícii. Toto ustanovenie treba vykladať so zreteľom na zásady prijateľnosti a zodpovednosti. Prevádzkovateľ nesmie zničiť informácie o zdroji údajov s cieľom získať výnimku, pokiaľ ide o ich zverejnenie, ani nesmie ignorovať zvyčajné štandardné a uznávané potreby dokumentácie v oblasti jeho činnosti. Ak prevádzkovateľ nebude viesť dokumentáciu o zdroji spracúvaných údajov, zvyčajne nesplní svoje povinnosti vyplývajúce z práva prístupu.

V prípade vykonávania automatizovaných hodnotení bude potrebné vysvetliť celkovú logiku hodnotenia vrátane jednotlivých kritérií, ktoré boli zohľadnené pri hodnotení dotknutej osoby.

V smernici sa nevysvetľuje, či sa právo prístupu k informáciám týka minulosti a ak áno, ktorého obdobia. V tejto súvislosti (ako sa zdôrazňuje v judikatúre SDEÚ) sa právo prístupu k údajom nesmie neprimerane obmedzovať časovými obmedzeniami. Dotknuté osoby musia tiež dostať vhodnú príležitosť, aby získali informácie o minulých operáciách spracovania údajov.

Príklad: SDEÚ mal vo veci *Rijkeboer*[179] určiť, či podľa článku 12 písm. a) smernice môže byť právo prístupu jednotlivca k informáciám o príjemcoch alebo kategóriách príjemcov osobných údajov a o obsahu oznámených údajov obmedzené na jeden rok pred podaním žiadosti o prístup.

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

Súdny dvor sa rozhodol, že pri určení toho, či článok 12 písm. a) smernice oprávňuje takéto časové obmedzenie, vyloží predmetný článok z hľadiska cieľov smernice. Najprv konštatoval, že právo prístupu je nevyhnutne potrebné s cieľom umožniť dotknutej osobe, aby mohla vykonať svoje právo úpravy, vymazania alebo zablokovania údajov prevádzkovateľom (článok 12 písm. b)) alebo oznámiť tretím stranám, ktorým sa tieto údaje zverejnili, uskutočnenie úpravy, vymazania alebo zablokovania (článok 12 písm. c)). Právo prístupu je takisto nevyhnutne potrebné s cieľom umožniť dotknutej osobe, aby vykonala svoje právo námietky proti spracovaniu jej osobných údajov (článok 14) a právo na súdny opravný prostriedok v prípade, že utrpí škodu (články 22 a 23).

Súdny dvor 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."

Právo úpravy, vymazania a zablokovania údajov

„Akákoľvek osoba musí byť schopná uplatniť právo prístupu k údajom, ktoré sa jej týkajú a ktoré sa spracúvajú, zvlášť kvôli overeniu presnosti údajov a zákonnosti spracovania."[180] V súlade s týmito zásadami sa musí vo vnútroštátnych právnych predpisoch dotknutým osobám zaručiť právo úpravy, vymazania alebo zablokovania ich údajov prevádzkovateľom, ak sa domnievajú, že spracúvanie ich údajov nie je v súlade s ustanoveniami smernice, predovšetkým z dôvodu nepresnosti alebo neúplnosti údajov[181].

Príklad: ESĽP vo veci *Cemalettin Canli/Turecko*[182] zistil porušenie článku 8 EDĽP v rámci nesprávnych hlásení 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

180 Smernica o ochrane údajov, odôvodnenie 41.

181 Tamtiež, článok 12 písm. b).

182 ESĽP, *Cemalettin Canli/Turecko*, č. 22427/04, 18. novembra 2008, odseky 33, 42 a 43; ESĽP, *Dalea/Francúzsko,* č. 964/07, 2. februára 2010.

správu s názvom *Informačný formulár o ďalších trestných činoch*, ktorý vyvolával dojem, že sťažovateľ je členom dvoch ilegálnych organizácií. Žiadosť sťažovateľa o zmenu správy a policajných záznamov nebola úspešná. ESĽP potvrdil, že informácie v policajnej správe boli v rozsahu pôsobnosti článku 8 EDĽP, keďže verejné informácie by takisto mohli patriť pod pojem „súkromný život", ak boli systematicky zbierané a uchovávané v súboroch držaných verejnými orgánmi. Okrem toho policajná správa nebola správna a jej vypracovanie a predloženie trestnému súdu nebolo v súlade s právnymi predpismi. Súd dospel k záveru, že došlo k porušeniu článku 8.

Príklad: Sťažovatelia vo veci *Segerstedt-Wiberg a iní/Švédsko*[183] boli priaznivcami určitých liberálnych a komunistických politických strán. Mali podozrenie, že informácie o nich boli zaznamenané do tajných policajných záznamov. ESĽP vyjadril uspokojenie nad tým, že uchovávanie predmetných údajov malo právny základ a legitímny cieľ. Pokiaľ ide o niektorých sťažovateľov, ESĽP konštatoval, že ďalšie uchovávania údajov predstavovalo neprimeraný zásah do ich súkromného života. Napríklad v prípade pána Schmida orgány uchovávali informácie o tom, že v roku 1969 údajne obhajoval násilný odpor proti policajnej kontrole počas demonštrácií. ESĽP zistil, že tieto informácie nesúviseli so žiadnym relevantným bezpečnostným záujmom, predovšetkým vzhľadom na ich historickú povahu. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP v prípade štyroch z piatich sťažovateľov.

V niektorých prípadoch postačí, ak dotknutá osoba požiada o úpravu napríklad písanej podoby mena, zmenu adresy alebo telefónneho čísla. Ak sa však takéto žiadosti týkajú právnych záležitostí, napríklad právnej totožnosti alebo správneho bydliska na účely doručovania právnych dokumentov, žiadosti o úpravu nemusia stačiť a prevádzkovateľ môže mať právo požadovať dôkaz o údajnej nepresnosti. Uvedená požiadavka nesmie dotknutú osobu zaťažiť neprimeraným dôkazným bremenom, a vylúčiť tak možnosť, aby dosiahla úpravu svojich údajov. ESĽP zistil porušenie článku 8 EDĽP v niekoľkých prípadoch, v ktorých sťažovateľ nedokázal spochybniť presnosť informácií uchovávaných v tajných registroch[184].

183 ESĽP, *Segerstedt-Wiberg a iní/Švédsko*, č. 62332/00, 6. júna 2006, odseky 89 a 90; pozri tiež napríklad ESĽP, *M. K./Francúzsko*, č. 19522/09, 18. apríla 2013.

184 ESĽP, *Rotaru/Rumunsko*, č. 28341/95, 4. Mája 2000.

Príklad: Vo veci *Ciubotaru/Moldavsko*[185] 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 doložiť. ESĽP uznal za prípustné, aby štáty požadovali objektívny dôkaz pri registrácii etnického pôvodu jednotlivca. Keby sa takýto nárok zakladal výlučne na subjektívnych a nedoložených základoch, orgány by mohli 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, sklony 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 predstavovala takáto požiadavka neprekonateľnú prekážku pre registráciu inej etnickej totožnosti než tej, ktorú zapísali rodičom sťažovateľa sovietske orgány. Štát bránil sťažovateľovi v tom, aby bol jeho nárok preskúmaný 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 EDĽP.

Dotknutá osoba môže v rámci občianskoprávneho konania alebo konania pred verejným orgánom s cieľom rozhodnúť o správnosti či nesprávnosti údajov požiadať o to, aby bol do jej spisu zanesený záznam alebo poznámka o spochybnení správnosti a o tom, že zatiaľ nebolo prijaté oficiálne rozhodnutie. V tomto období prevádzkovateľ nesmie údaje predstavovať ako určité či konečné, najmä vo vzťahu k tretím stranám.

Žiadosť dotknutej osoby o výmaz údajov sa často zakladá na tvrdení, že spracovanie údajov nemá legitímny základ. Takého nároky často vnikajú po zrušení súhlasu alebo vtedy, keď určité údaje už nie sú potrebné na dosiahnutie účelu zberu údajov. Dôkazné bremeno týkajúce sa legitímnosti spracúvania údajov sa presunie na prevádzkovateľa, keďže on je zodpovedný za legitímnosť spracúvania. Podľa zásady zodpovednosti musí byť prevádzkovateľ kedykoľvek schopný preukázať, že existuje pevný právny základ pre dané spracúvanie údajov, v opačnom prípade sa spracúvanie musí zastaviť.

Ak je spracovanie údajov spochybnené buď z dôvodu nesprávnosti údajov, alebo nezákonnosti ich spracovania, dotknutá osoba môže v súlade so zásadou prijateľného spracúvania požadovať zablokovanie sporných údajov. To znamená, že údaje

185 ESĽP, *Ciubotaru/Moldavsko*, č. 27138/04, 27. apríla 2010, body 51 a 59.

nebudú vymazané, ale prevádzkovateľ sa musí zdržať ich používania v lehote zablokovania. To je nevyhnutné predovšetkým vtedy, keď by ďalšie používanie nepresných alebo nezákonne uchovávaných údajov mohlo poškodiť dotknutú osobu. Vo vnútroštátnych právnych predpisoch by sa malo spresniť, kedy môže vzniknúť povinnosť zablokovať používanie údajov a akým spôsobom by sa toto zablokovanie malo uskutočniť.

Dotknuté osoby majú ďalej právo získať od prevádzkovateľa oznámenie tretím stranám o zablokovaní, úprave alebo vymazaní, pokiaľ tretie strany prijali údaje pred uvedenými operáciami spracúvania. Keďže prevádzkovateľ je povinný zdokumentovať zverejnenie údajov tretím stranám, malo by byť možné identifikovať príjemcov údajov a požiadať ich o výmaz. Ak medzitým došlo k uverejneniu údajov, napríklad na internete, zrejme nebude možné vymazať údaje vo všetkým prípadoch, keďže sa nepodarí nájsť príjemcov údajov. Podľa smernice o ochrane údajov je kontaktovanie príjemcov údajov v súvislosti s úpravou, výmazom alebo zablokovaním údajov záväzné, „pokiaľ to nie je nemožné, alebo pokiaľ to nevyžaduje neprimerané úsilie“[186].

5.1.2. Právo námietky

Právo námietky zahŕňa právo námietky proti automatizovaným individuálnym rozhodnutiam, právo námietky z dôvodu konkrétnej situácie dotknutej osoby a právo námietky proti ďalšiemu používaniu údajov na účely priameho marketingu.

Právo námietky proti automatizovaným individuálnym rozhodnutiam

Automatizované rozhodnutia sú rozhodnutia prijaté s použitím osobných údajov spracúvaných výlučne automatickými prostriedkami. Ak je pravdepodobné, že tieto rozhodnutia budú mať zásadný vplyv na životy jednotlivcov, keďže sa týkajú napríklad ich úverovej bonity, pracovného výkonu, správania alebo spoľahlivosti, je nevyhnutná osobitná ochrana, ktorá zabráni neprimeraným dôsledkom. V smernici o ochrane údajov sa stanovuje, že automatizovanými rozhodnutiami sa nesmú posudzovať otázky, ktoré sú dôležité pre jednotlivcov, a vyžaduje, aby jednotlivec mal právo na revíziu automatizovaného rozhodnutia[187].

186 Smernica o ochrane údajov, článok 12 písm. c) druhá polovica vety.

187 Tamtiež, článok 15 ods. 1.

Príklad: Dôležitým praktickým príkladom automatizovaného rozhodnutia je bodové hodnotenie kreditného rizika. V záujme rýchleho rozhodnutia o úverovej bonite budúceho zákazníka sa zberajú určité údaje zákazníka, napríklad povolanie a rodinná situácia, a kombinujú sa s údajmi o danej osobe dostupnými z iných zdrojov, napríklad systémov informácií o úveroch. Zozbierané údaje sa automaticky zanesú do bodovacieho algoritmu, ktorým sa vypočíta celková hodnota predstavujúcu úverovú bonitu potenciálneho zákazníka. Na základe týchto informácií môže zamestnanec spoločnosti v priebehu niekoľkých sekúnd rozhodnúť, či je dotknutá osoba prijateľná ako zákazník alebo nie.

Členské štáty podľa smernice stanovujú, že sa na osobu môžu vzťahovať individuálne automatizované rozhodnutia v prípade, že sa netýkajú záujmov dotknutej osoby, keďže sa rozhodlo v jej prospech, alebo sú tieto záujmy zaručené inými vhodnými prostriedkami[188]. Právo námietky proti automatizovaným rozhodnutiam je takisto zahrnuté v **právnych predpisoch Rady Európy**, ako je zrejmé z odporúčania o profilovaní[189].

Právo námietky z dôvodu konkrétnej situácie dotknutej osoby

Neexistuje žiadne všeobecné právo námietky dotknutých osôb proti spracúvaniu ich údajov[190]. V článku 14 písm. a) smernice o ochrane údajov sa však dotknutej osobe udeľuje právomoc vzniesť námietku na základe nevyvrátiteľných zákonných dôvodov týkajúcich sa konkrétnej situácie dotknutej osoby. Podobné právo sa uznáva v odporúčaní Rady Európy o profilovaní[191]. Cieľom uvedených ustanovení je dosiahnuť rovnováhu medzi právom dotknutých osôb na ochranu údajov a legitímnymi právami iných na spracúvanie údajov dotknutých osôb.

Príklad: Banka uchováva sedem rokov údaje o zákazníkoch, ktorí nesplácajú včas splátky. Zákazník, ktorého údaje boli uložené v tejto databáze, požiada o novú pôžičku. Úradník nahliadne do databázy, zhodnotí finančnú situáciu zákazníka a zamietne poskytnutie pôžičky. Zákazník však môže namietať proti záznamu osobných údajov v databáze a požadovať o ich výmaz, ak je schopný

188 Tamtiež, článok 15 ods. 2.

189 Odporúčania o profilovaní, článok ods. 5.

190 Pozri tiež ESĽP, *M.S./Švédsko*, č. 20837/92, 27. augusta 1997, v tomto prípade boli oznámené zdravotné údaje bez súhlasu alebo možnosti námietky, alebo ESĽP, *Leander/Švédsko*, č. 9248/81, 26. marca 1987, alebo ESĽP, *Mosley/Spojené kráľovstvo*, č. 48009/08, 10. mája 2011.

191 Odporúčanie o profilovaní, článok 5 ods. 3.

dokázať, že príčinou oneskorenia splátok bola chyba, ktorú napravil bezprostredne po tom, ako sa o nej dozvedel.

Výsledkom úspešnej námietky je, že prevádzkovateľ nesmie ďalej spracúvať predmetné údaje. Operácie spracúvania vykonané na údajoch dotknutej osoby pred podaním námietky však zostanú legitímne.

Právo námietky proti ďalšiemu použitiu údajov na priame marketingové účely

V článku 14 písm. b) smernice o ochrane údajov sa stanovuje osobitné právo námietky proti použitiu údajov určitej osoby na účely priameho marketingu. Toto právo je zakotvené aj v odporúčaní Rady Európy o priamom marketingu[192]. Takýto druh námietky má byť vznesený pred sprístupnením údajov tretím stranám na účely priameho marketingu. Dotknuté osoby teda musia dostať možnosť vzniesť námietku pred prenosom údajov.

5.2. Nezávislý dohľad

Hlavné body

- V záujme zaistenia účinnej ochrany údajov musia byť na základe vnútroštátnych právnych predpisov zriadené nezávislé dozorné orgány.
- Vnútroštátne dozorné orgány musia byť úplne nezávislé, pričom ich nezávislosť musí byť zaručená v ustanovujúcom právnom predpise a vyjadrená v osobitnej organizačnej štruktúre dozorného orgánu.
- Dozorné orgány majú osobitné úlohy zahŕňajúce okrem iného:
  - monitorovanie a podporu ochrany údajov na vnútroštátnej úrovni;
  - poskytovanie poradenstva dotknutým osobám a prevádzkovateľom, ako aj štátnej správe a širšej verejnosti;
  - prijímanie sťažností a pomoc dotknutým osobám v prípadoch podozrenia na porušenie práv na ochranu údajov;
  - vykonávanie dohľadu nad prevádzkovateľmi a sprostredkovateľmi;

192 Rada Európy, Výbor ministrov (1985), odporúčanie členským štátom č. Rec(85)20 o ochrane osobných údajov používaných na účely priameho marketingu, 25. októbra 1985, článok 4, ods. 1.

- v prípade potreby zasahovanie formou
  - výstrahy, napomenutia, a dokonca udelenia pokuty prevádzkovateľom a sprostredkovateľom,
  - vydania príkazu na úpravu, zablokovanie alebo výmaz údajov,
  - vydania zákazu spracúvania;
- postupovanie vecí k súdu.

V smernici o ochrane údajov sa vyžaduje nezávislý dozor ako dôležitý mechanizmus na zaistenie účinnej ochrany údajov. V smernici sa zavádza nástroj na presadzovanie ochrany údajov, ktorý nebol zahrnutý ani do dohovoru č. 108, ani do usmernení OECD týkajúcich sa ochrany súkromia.

Vzhľadom na to, že nezávislý dozor sa osvedčil ako nenahraditeľná záruka účinnej ochrany údajov, v novom ustanovení revidovaných usmernení OECD týkajúcich sa ochrany súkromia z roku 2013 sa členské štáty vyzývajú, aby „zriadili a zachovávali orgány na presadzovanie ochrany súkromia, ktoré budú mať odborné poznatky v oblasti spravovania, zdrojov a techniky nevyhnutne potrebné na vykonávanie zverených právomocí a prijímanie objektívnych, nestranných a konzistentných rozhodnutí“[193].

V rámci právnych predpisov Rady Európy sa povinnosť zriadiť dozorné orgány stanovuje v dodatkovom protokole k dohovoru č. 108. Uvedený nástroj obsahuje v článku 1 právny rámec pre nezávislé dozorné orgány, ktorý zmluvné strany musia vykonávať v rámci vnútroštátnych právnych predpisov. V ustanovení sú opísané úlohy a právomoci dozorných orgánov podobnými formuláciami ako smernica o ochrane údajov. Dozorné orgány by teda mali podľa právnych ustanovení EÚ a Rady Európy v podstate fungovať rovnako.

V rámci právnych predpisov EÚ boli kompetencie a organizačná štruktúra dozorných orgánov prvýkrát načrtnuté v článku 28 ods. 1 smernice o ochrane údajov. V nariadení o ochrane údajov inštitúciami EÚ[194] sa zriaďuje funkcia európskeho dozorného úradníka pre ochranu údajov ako orgánu, ktorý má dohliadať na spracúvanie údajov

193 OECD (2013), Usmernenia o riadení ochrany súkromia a cezhraničných tokov osobných údajov, článok 19 písm. c).

194 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, články 41–48.

orgánmi a inštitúciami EÚ. V nariadení sa opisujú úlohy a zodpovednosť dozorného orgánu a vychádza sa pri tom zo skúseností zhromaždených od uverejnenia smernice o ochrane údajov.

Nezávislosť orgánov pre ochranu údajov je zaručená článkom 16 ods. 2 ZFEÚ a článkom 8 ods. 3 charty. V poslednom ustanovení sa osobitne zdôrazňuje, že kontrola nezávislým orgánom je najdôležitejšou zložkou základného práva na ochranu údajov. V smernici o ochrane údajov sa okrem toho vyžaduje, aby členské štáty zriadili úplne nezávisle pôsobiace dozorné orgány na monitorovanie vykonávania smernice[195]. Právny predpis, ktorý je základom vytvorenia dozorného orgánu, musí nielen obsahovať ustanovenia, ktoré osobitne zaručia jeho nezávislosť, ale nezávislosť musí byť zrejmá aj z osobitnej organizačnej štruktúry orgánu.

V roku 2010 sa SDEÚ prvýkrát zaoberal otázkou rozsahu požiadavky na nezávislosť dozorných orgánov pre ochranu údajov[196]. Závery Súdneho dvora ilustrujú nasledujúce príklady.

Príklad: Vo veci *Komisia/Nemecko*[197] 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 spracovania osobných údajov mimo verejného sektora v rôznych spolkových krajinách (*Länder*).

Podľa Súdneho dvora posúdenie dôvodnosti predmetnej veci záviselo od rozsahu požiadavky nezávislosti obsiahnutej v uvedenom ustanovení, a teda od výkladu tohto ustanovenia.

Súdny dvor zdôraznil, že výklad výrazu „úplne nezávisle" v článku 28 ods. 1 smernice musí zohľadniť samotné znenie uvedeného ustanovenia, ako aj ciele a systematiku smernice o ochrane údajov[198]. Poukázal na to, že dozorné orgány

195 Smernica o ochrane údajov, článok 28 ods. 1 posledná veta; Dohovor č. 108, dodatkový protokol, článok 1 ods. 3.

196 Pozri FRA (2010), *Základné práva: výzvy a úspechy v roku 2010*, výročná správa za rok 2010, s. 59. Agentúra FRA sa touto otázkou podrobnejšie zaoberá vo svojej správe na tému *Ochrana údajov v Európskej únii: úloha vnútroštátnych orgánov na ochranu údajov*, ktorá bola uverejnená v máji 2010.

197 SDEÚ, C-518/07, *Európska komisia/Spolková republika Nemecko*, 9. marca 2010, bod 27.

198 Tamtiež, body 17 a 29.

sú „strážcovia" základných práv týkajúcich sa spracovania osobných údajov zaručených smernicou a ich zriadenie v členských štátoch je považované „za nevyhnutný prvok ochrany jednotlivcov v súvislosti so spracovaním osobných údajov"[199]. Súdny dvor dospel k záveru, že „pri vykonávaní svojich úloh musia dozorné orgány konať objektívne a nestranne. 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"[200].

SDEÚ takisto konštatoval, že význam výrazu „úplná nezávislosť" by sa mal vykladať so zreteľom na nezávislosť európskeho dozorného úradníka pre ochranu údajov, ako je vymedzená v nariadení o ochrane údajov inštitúciami EÚ. Ako zdôraznil Súdny dvor, v článku 44 ods. 2 uvedeného nariadenia sa vysvetľuje pojem nezávislosti tak, že sa dodáva, že „európsky dozorný úradník pre ochranu údajov pri výkone svojich služobných povinností od nikoho nežiada ani neprijíma pokyny". Tým sa vylučuje štátny dohľad nad nezávislým dozorným orgánom na ochranu údajov[201].

V súlade s tým SDEÚ skonštatoval, že nemecké inštitúcie pre ochranu údajov na spolkovej úrovni, zodpovedné za monitorovanie spracovania osobných údajov neverejnými orgánmi, neboli dostatočne nezávislé, keďže boli podrobené dohľadu zo strany štátu.

Príklad: Vo veci *Komisia/Rakúsko*[202] SDEÚ poukázal na podobné problémy týkajúce sa postavenia určitých členov a zamestnancov rakúskeho úradu pre ochranu údajov (Komisia pre ochranu údajov, DSK). Súd dospel k záveru, že v tomto prípade rakúske právne predpisy neumožňovali rakúskemu úradu pre ochranu údajov, aby plnil svoju funkciu úplne nezávisle v zmysle smernice o ochrane údajov. Nezávislosť rakúskeho úradu pre ochranu údajov nebola dostatočne zaručená, keďže spolková kancelária poskytovala komisii DSK svojich zamestnancov, dohliadala na ňu a mala právo na nepretržité informácie o jej činnosti.

199 Tamtiež, bod 23.

200 Tamtiež, bod 25.

201 Tamtiež, bod 27.

202 SDEÚ, C-614/10, *Európska komisia/Rakúska republika*, 16. októbra 2012, body 59 a 63.

Príklad: Vo veci *Komisia/Maďarsko*[203] 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". Súd rozhodol, že „Maďarsko si predčasným ukončením funkčného obdobia dozorného orgánu pre ochranu osobných údajov nesplnilo povinnosti, ktoré mu vyplývajú zo smernice Európskeho parlamentu a Rady 95/46/ES [...]."

Dozorné orgány majú podľa vnútroštátnych právnych predpisov právomoci a funkcie zahŕňajúce okrem iného:[204]

- poskytovanie poradenstva prevádzkovateľom a dotknutým osobám vo všetkých otázkach týkajúcich sa ochrany údajov;
- vyšetrovanie operácií spracúvania a zasahovanie príslušným spôsobom;
- varovanie alebo napomínanie prevádzkovateľov;
- nariaďovanie úpravy, vymazania a zablokovania či zničenia údajov;
- vydávanie dočasných alebo trvalých zákazov spracúvania;
- postupovanie vecí k súdu.

Aby dozorný orgán dokázal plniť stanovené úlohy, musí mať prístup ku všetkým osobným údajom a informáciám nevyhnutne potrebným na prešetrovanie, ako aj prístup do všetkých priestorov, v ktorých prevádzkovateľ uchováva relevantné informácie.

Existujú zásadné rozdiely medzi domácimi jurisdikciami, pokiaľ ide o postupy a právne dôsledky zistení dozorných orgánov. Môže ísť o odporúčania typu ombudsmana až po okamžite vykonateľné rozhodnutia. Preto je pri analýze efektívnosti prostriedkov nápravy dostupných v určitej jurisdikcii nutné posudzovať tieto prostriedky v príslušnom kontexte.

203 SDEÚ, C-288/12, *Európska komisia/Maďarsko*, 8. apríla 2014, body 50 a 67.

204 Smernica o ochrane údajov, článok 28; ďalej pozri dohovor č. 108, dodatkový protokol článok 1.

5.3. Prostriedky nápravy a sankcie

Hlavné body

- Podľa dohovoru č. 108, ako aj podľa smernice o ochrane údajov, sa musia vo vnútroštátnych právnych predpisoch stanoviť príslušné prostriedky nápravy a sankcie v prípade porušenia práva na ochranu údajov.
  - Právo na účinný prostriedok nápravy podľa právnych predpisov EÚ si vyžaduje, aby sa vo vnútroštátnych právnych predpisoch stanovili opravné prostriedky proti porušeniu práv v oblasti ochrany údajov, a to bez ohľadu na možnosť obrátiť sa na dozorný orgán.
  - Vo vnútroštátnych právnych predpisoch sa musia stanoviť sankcie, ktoré sú účinné, rovnocenné, primerané a odrádzajúce.
- Skôr než sa osoba obráti na súd, musí kontaktovať prevádzkovateľa. To, či je alebo nie je záväzné obrátiť sa na dozorný orgán pred podaním súdnej žaloby upravujú vnútroštátne právne predpisy.
- Dotknuté osoby sa môžu v prípade porušenia právnych predpisov o ochrane údajov obrátiť ako na poslednú inštanciu a za určitých podmienok na ESĽP.
- Dotknuté osoby sa môžu obrátiť aj na SDEÚ, ale len vo veľmi obmedzenej miere.

Práva vyplývajúce z právnych predpisov na ochranu údajov môže uplatňovať len osoba, o ktorej práva ide, teda osoba, ktorá je (alebo si aspoň nárokuje, že je) dotknutou osobou. Takéto osoby môžu byť pri uplatňovaní svojich práv zastúpené inými osobami spĺňajúcimi nevyhnutné podmienky stanovené vnútroštátnymi právnymi predpismi. Maloleté osoby musia zastupovať ich rodičia alebo poručníci. Pred dozorným orgánom môžu danú osobu zastupovať aj združenia, ktorých zákonným cieľom je podporovať práva na ochranu údajov.

5.3.1. Požiadavky na prevádzkovateľa

Práva uvedené v oddiele 3.2 sa najprv musia vykonávať vo vzťahu k prevádzkovateľovi. Obrátiť sa priamo na vnútroštátny dozorný orgán alebo súd nepomôže, keďže dozorný orgán môže dotknutej osobe poradiť len to, aby sa najskôr obrátila na prevádzkovateľa, a súd označí sťažnosť za neprípustnú. Formálne požiadavky na právne relevantnú žiadosť na prevádzkovateľa, najmä to, či žiadosť musí byť písomná, sa majú regulovať vnútroštátnymi právnymi predpismi.

Subjekt, ktorý bol oslovený ako prevádzkovateľ, musí na žiadosť reagovať, a to dokonca aj vtedy, ak nie je prevádzkovateľom. Odpoveď musí byť v každom prípade doručená dotknutej osobe v lehote predpísanej vnútroštátnymi právnymi predpismi, a to aj vtedy, keby obsahovala len oznámenie o tom, že sa nespracúvajú žiadne údaje žiadateľa. V súlade s ustanoveniami článku 12 písm. a) smernice o ochrane údajov a článku 8 písm. b) dohovoru č. 108 musí byť žiadosť spracovaná „bez prílišného zdržiavania". Vo vnútroštátnych právnych predpisoch by preto mala byť predpísaná lehota na zaslanie odpovede, ktorá je dostatočne krátka, zároveň však umožňuje prevádzkovateľovi, aby sa žiadosťou primerane zaoberal.

Skôr než subjekt oslovený ako prevádzkovateľ odpovie na žiadosť, musí potvrdiť totožnosť žiadateľa, aby mohol určiť, či skutočne ide o osobu uvedenú v žiadosti, a predísť tak závažnému porušeniu dôvernosti. Ak sa vo vnútroštátnych právnych predpisoch požiadavky na potvrdenie totožnosti osobitne neupravujú, musí o nich rozhodnúť prevádzkovateľ. Zásada prijateľného spracúvania si však vyžaduje, aby prevádzkovatelia nepredpisovali príliš náročné podmienky potvrdenia totožnosti (a pravosti žiadosti, ako je opísané v oddiele 2.1.1).

Vo vnútroštátnych právnych predpisoch sa tiež musí vyriešiť, či prevádzkovatelia smú alebo nesmú požadovať uhradenie poplatku od žiadateľa pred vybavením žiadosti. V súlade s ustanoveniami článku 12 písm. a) smernice o ochrane údajov a článku 8 písm. b) dohovoru č. 108 musí byť odpoveď na žiadosť o prístup vybavená „bez [prílišných] výdavkov". Vo vnútroštátnych právnych predpisoch mnohých európskych krajín sa stanovuje, že odpovede na žiadosti, na ktoré sa vzťahujú právne predpisy o ochrane údajov, musia byť bezplatné, ak si nevyžadujú nadmerné a nezvyčajné úsilie. Na druhej strane sú prevádzkovatelia zvyčajne chránení vnútroštátnymi právnymi predpismi pred zneužitím práva na odpoveď na žiadosť.

Ak osoba, inštitúcia alebo orgán, ktoré boli oslovené ako prevádzkovatelia, nepopierajú, že sú prevádzkovateľmi, musia v lehote predpísanej vnútroštátnymi právnymi predpismi:

- pristúpiť k žiadosti a oznámiť žiadajúcej osobe, akým spôsobom sa žiadosti vyhovelo alebo

- informovať žiadateľa o tom, prečo sa jeho žiadosti nevyhovelo.

5.3.2. Sťažnosti predložené dozornému orgánu

Ak osoba, ktorá požiadala o prístup alebo vzniesla námietku proti prevádzkovateľovi, nedostane včasnú a uspokojivú odpoveď, môže sa obrátiť so žiadosťou o pomoc na vnútroštátny dozorný orgán pre ochranu údajov. V rámci konania vedeného dozorným orgánom by sa malo ozrejmiť, či osoba, inštitúcia alebo orgán oslovené žiadateľom boli skutočne povinné reagovať na žiadosť a či táto reakcia bola správna a dostatočná. Dozorný orgán musí informovať príslušnú osobu o výsledku konania v jej veci[205]. Právne dôsledky konaní vedených vnútroštátnymi dozornými orgánmi závisia od vnútroštátnych právnych predpisov: či je podľa nich možné právne vykonávať rozhodnutia dozorného orgánu v tom zmysle, či sú vynútiteľné úradným orgánom, alebo či je nevyhnutné podať súdnu žalobu v prípade, že prevádzkovateľ nerešpektuje rozhodnutie dozorného orgánu (stanovisko, napomenutie atď.).

V prípade podozrenia na porušenie práv na ochranu údajov zaručených článkom 16 ZFEÚ inštitúciami alebo orgánmi EÚ môže dotknutá osoba podať sťažnosť európskemu dozornému úradníkovi pre ochranu údajov[206], teda nezávislému dozornému orgánu pre ochranu údajov podľa nariadenia o ochrane údajov inštitúciami EÚ, ktorým sa vymedzujú povinnosti a právomoci uvedeného úradníka. Ak európsky dozorný úradník pre ochranu údajov neodpovie do šiestich mesiacov, sťažnosť treba pokladať za zamietnutú.

Musí existovať možnosť súdneho odvolania proti rozhodnutiam vnútroštátneho dozorného orgánu. Týka sa to dotknutých osôb, ako aj prevádzkovateľov, ktorí boli stranami konania vedeného dozorným orgánom.

Príklad: Komisia Spojeného kráľovstva pre informácie vydala 24. júla 2013 rozhodnutie, ktorým požiadala políciu v kraji Hertfordshire, aby prestala používať systém sledovania poznávacích značiek vozidiel, ktorý komisia pokladala za nezákonný. Údaje zozbierané kamerami sa uchovávali v miestnych policajných databázach a v centralizovanej databáze. Fotografie poznávacích značiek sa uchovávali dva roky a fotografie vozidiel 90 dní. Komisia konštatovala, že takéto rozsiahle používanie kamier a ďalších foriem sledovania nebolo primerané problému, ktorý sa snažilo vyriešiť.

205 Smernica o ochrane údajov, článok 28 ods. 4.

206 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.

5.3.3. Súdne žaloby

Podľa smernice o ochrane údajov platí, že ak osoba, ktorá sa obrátila na prevádzkovateľa so žiadosťou v súlade s právnymi predpismi o ochrane údajov, nie je spokojná s jeho odpoveďou, musí mať nárok na podanie žaloby na vnútroštátnom súde[207].

To, či je alebo nie je záväzné obrátiť sa na dozorný orgán pred podaním súdnej žaloby, sa upravuje vo vnútroštátnych právnych predpisoch. V každom prípade bude výhodné, ak sa osoby vykonávajúce svoje práva na ochranu údajov najskôr obrátia na dozorný orgán, keďže konania so žiadosťami o pomoc by nemali byť príliš byrokratické a mali by byť bezplatné. Dotknutej osobe by pri presadzovaní príslušných práv na súde mohla pomôcť expertíza zdokumentovaná v rozhodnutiach dozorného orgánu (stanovisko, napomenutie atď.).

Podľa právnych predpisov Rady Európy je v prípade porušenia práv na ochranu údajov, ku ktorému údajne došlo na vnútroštátnej úrovni zmluvnej strany EDĽP a ktoré zároveň predstavuje porušenie článku 8 EDĽP, možné podať žalobu na ESĽP, a to po vyčerpaní všetkých dostupných domácich prostriedkov nápravy. Žaloba vo veci porušenia článku 8 EDĽP musí tiež spĺňať kritériá prípustnosti (články 34 – 37 EDĽP)[208].

Aj keď sa sťažnosti na ESĽP môžu týkať len zmluvných strán, nepriamo môžu súvisieť s konaním alebo opomenutím súkromných strán, a to do tej miery, do akej zmluvná strana nesplnila svoje povinnosti konať vyplývajúce z EDĽP a nezaistila dostatočnú ochranu pred porušením práv na ochranu údajov v rámci svojich vnútroštátnych právnych predpisov.

Príklad: Vo veci *K. U./Fínsko*[209] sa maloletý sťažovateľ sťažoval, že na internetovej stránke umožňujúcej zoznámenie bol o ňom uverejnený inzerát sexuálnej povahy. Poskytovateľ služieb nezverejnil totožnosť osoby, ktorá informácie umiestnila, z dôvodu záväzku dôvernosti vyplývajúceho z fínskych právnych predpisov. Sťažovateľ tvrdil, že fínske právne predpisy mu neposkytli dostatočnú ochranu pred krokmi súkromných osôb, ktoré umiestnili na internete inkriminujúce údaje o sťažovateľovi. ESĽP konštatoval, že štáty sú nielen

207 Smernica o ochrane údajov, článok 22.

208 ESĽP, články 34–37, dostupné na adrese: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 EDĽP, *K.U./Fínsko*, č. 2872/02, 2. marca 2009.

povinné zdržať sa svojvoľného zasahovania do súkromného života jednotlivcov, ale môžu mať aj povinnosti konať , ktoré zahŕňajú „prijatie opatrení určených na zabezpečenie rešpektovania súkromného života dokonca aj vo sfére vzájomných vzťahov jednotlivcov". Praktická a účinná ochrana sťažovateľa v tomto prípade si vyžadovala prijatie účinných opatrení na určenie a stíhanie páchateľa. Štát však takúto ochranu nezabezpečil a ESĽP dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

Príklad: Sťažovateľka vo veci *Köpke/Nemecko*[210] čelila podozreniu z krádeže na pracovisku, a preto bola tajne sledovaná prostredníctvom videozáznamu. ESĽP dospel k záveru, že „nič nenaznačuje, že by domáce orgány neusilovali o dosiahnutie rovnováhy, v rámci priestoru pre 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.

Ak ESĽP zistí, že štát, ktorý je zmluvnou stranou EDĽP, porušil niektoré z práv chránených EDĽP, je povinný vykonať rozsudok ESĽP. Vykonávacími opatreniami sa musí najskôr ukončiť porušovanie a musia sa napraviť (v maximálnej možnej miere) negatívne dôsledky porušovania týkajúce sa 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 EDĽP, podľa článku 41 môže poškodenej strane priznať spravodlivé zadosťučinenie na náklady štátu.

Podľa právnych predpisov EÚ[211] môžu obete porušovania vnútroštátnych právnych predpisov o ochrane údajov, ktorými sa vykonávajú právne predpisy EÚ o ochrane údajov, v určitých prípadoch podať žalobu k SDEÚ. Existujú dva spôsoby, ako môže sťažnosť dotknutej osoby na porušenie jej práv na ochranu údajov viesť k začatiu konania na SDEÚ.

210 ESĽP, *Köpke/Nemecko* (dec.), č. 420/07, 5. októbra 2010.

211 EÚ (2007), Lisabonská zmluva, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva, podpísaná v Lisabone 13. decembra 2007, Ú. v. EÚ C 306, 2007. Pozri tiež konsolidované verzie Zmluvy o Európskej únii, Ú. v. EÚ C 326, 2012 a ZFEÚ, Ú. v. EÚ C 326, 2012.

V rámci prvej možnosti by dotknutá osoba musela byť priamou obeťou správneho alebo regulačného opatrenia, ktorým sa porušuje právo jednotlivca na ochranu údajov. Podľa článku 263 ods. 4 ZFEÚ:

> *„Akákoľvek fyzická alebo právnická osoba môže [...] podať žalobu proti aktom, ktoré sú jej určené alebo ktoré sa jej priamo a osobne týkajú, ako aj voči regulačným aktom, ktoré sa jej priamo týkajú a nevyžadujú vykonávacie opatrenia."*

Obete nezákonného spracúvania údajov orgánom EÚ sa teda môžu obrátiť priamo na Všeobecný súd SDEÚ, ktorý predstavuje orgán Súdneho dvora s právomocou prijímať rozsudky vo veciach, na ktoré sa vzťahuje nariadenie o ochrane údajov inštitúciami EÚ. Existuje aj možnosť podania žaloby priamo k SDEÚ v prípade, že právne ustanovenie EÚ priamo ovplyvňuje právne postavenie určitej osoby.

Druhá možnosť sa týka právomoci SDEÚ (Súdny dvor) vydávať predbežné nálezy podľa článku 267 ZFEÚ.

Dotknuté osoby sa môžu v rámci domácich konaní obrátiť na vnútroštátny súd, aby požiadal Súdny dvor o vysvetlenie výkladu zmlúv EÚ, ako aj o výklad a potvrdenie platnosti opatrení inštitúcií, orgánov, úradov alebo agentúr EÚ. Takéto vysvetlenia sa nazývajú predbežné nálezy. Nejde o priamy prostriedok nápravy pre sťažovateľa, ale umožňujú vnútroštátnym súdom uplatňovať správny výklad právnych predpisov EÚ.

Ak strana sporu na vnútroštátnom súde požaduje postúpenie otázky SDEÚ, povinnosť postúpiť otázku sa týka len tých vnútroštátnych súdov, ktoré sú najvyššími inštanciami a proti ich rozhodnutiu nie je prípustný opravný prostriedok.

Príklad: Rakúsky ústavný súd vo veci *Kärntner Landesregierung a iní*[212] položil otázku SDEÚ týkajúcu sa platnosti článkov 3 až 9 smernice 2006/24/ES (*smernica o uchovávaní údajov*) so zreteľom na články 7, 9a 11 charty a o tom, 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.

212 SDEÚ, Spojené veci C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a iní*, 8. apríla 2014.

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 odosielal a prijímal, teda prechádzali cez verejné telekomunikačné siete. Podľa rakúskeho zákona o telekomunikáciách z roku 2003 je jeho poskytovateľ telekomunikačných služieb zo zákona povinný zbierať a uchovávať údaje o tom, ako používa sieť. Pán Seitlinger sa domnieval, že takýto zber a uchovávanie osobných údajov vôbec nebolo nevyhnutné na technické účely získania informácií z A do B po sieti. Podobne nebolo nevyhnutné zbieranie a uchovávanie údajov (dokonca vzdialene) na účely fakturácie. Pán Seitlinger určite neposkytol súhlas s takýmto používaním svojich osobných údajov. Jediným dôvodom zberu a uchovávania všetkých dodatočných údajov bol rakúsky zákon o telekomunikáciách z roku 2003.

Pán Seitlinger sa preto obrátil na rakúsky ústavný súd, kde tvrdil, že štatutárne povinnosti jeho poskytovateľa telekomunikačných služieb porušujú jeho základné práva vyplývajúce z článku 8 charty.

Súdny dvor prijal rozhodnutie len o podstatných zložkách žiadosti o predbežný nález v postúpenej veci. Právomoc rozhodnúť v pôvodnom prípade ponechal na vnútroštátnom súde.

Súdny dvor musí v zásade odpovedať na otázky, ktoré mu boli položené. Nemôže odmietnuť vydať predbežný nález s odôvodnením, že odpoveď by buď nebola relevantná, alebo by nebola vhodne načasovaná vzhľadom k pôvodnému prípadu. Odmietnuť však môže v prípade, že otázka nepatrí do rozsahu jeho pôsobnosti.

Napokon, ak existuje podozrenie na porušenie práv na ochranu údajov zaručených článkom 16 ZFEÚ zo strany inštitúcie alebo orgánu EÚ pri spracovaní osobných údajov, dotknutá osoba sa môže obrátiť na Všeobecný súd SDEÚ (článok 32 ods. 1 a 4 nariadenia o ochrane údajov inštitúciami EÚ). To sa týka aj rozhodnutí európskeho dozorného úradníka pre ochranu údajov o porušeniach (článok 32 ods. 3 nariadenia o ochrane údajov inštitúciami EÚ).

Všeobecný súd SDEÚ má síce právomoc rozhodovať vo veciach patriacich do rozsahu pôsobnosti nariadenia o ochrane údajov inštitúciami EÚ, ak sa však o dosiahnutie nápravy usiluje osoba, ktorá je zamestnancom inštitúcie alebo orgánu EÚ, musí sa obrátiť na Súd pre verejnú službu Európskej únie.

Príklad: Dostupné prostriedky nápravy proti činnostiam alebo rozhodnutiam inštitúcií a orgánov EÚ týkajúcim sa ochrany údajov ilustruje vec *Európska komisia/The Bavarian Lager Co. Ltd*[213].

Spoločnosť Bavarian Lager 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 prednostných záujmov ochrany údajov[214]. 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, *Bavarian Lager/Komisia*, zrušil rozhodnutie Komisie o zamietnutí žiadosti o prístup. Európska komisia sa proti rozsudku odvolala k Súdnemu dvoru EÚ. Veľká komora Súdneho dvora vyniesla rozsudok, ktorým zrušila rozsudok Súdu prvého stupňa a potvrdila zamietnutie žiadosti o prístup Európskou komisiou.

5.3.4. Sankcie

V rámci právnych predpisov Rady Európy sa v článku 10 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. 108215. **V rámci právnych predpisov EÚ sa** v článku 24 smernice o ochrane údajov ukladá, že členské štáty „prijmú vhodné opatrenia na zabezpečenie úplného zavedenia ustanovení tejto smernice a najmä ustanovia sankcie, ktoré sa uvalia v prípade porušenia ustanovení prijatých […]".

Oba nástroje poskytujú členským štátom široký priestor pre vlastné uváženie pri výbere vhodných sankcií a opravných prostriedkov. Ani v jednom právnom nástroji sa neuvádzajú konkrétne usmernenia týkajúce sa povahy alebo typu primeraných sankcií, ani príklady sankcií.

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

214 Analýzu argumentácie pozri: (EDPS) (2011), *Verejný prístup k dokumentom obsahujúcim osobné údaje po vynesení rozsudku Bavarian Lager*, Brusel, EDPS, dostupné na adrese: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

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

Ale:

> *„hoci členské štáty EÚ majú široký priestor pre vlastné uváženie pri určovaní najvhodnejších opatrení s cieľom zaručiť práva, ktoré pre jednotlivcov vyplývajú z právnych predpisov EÚ, v súlade so zásadou lojálnej spolupráce stanovenou v článku 4 ods. 3 ZEÚ, mali by rešpektovať minimálne požiadavky účinnosti, rovnocennosti, primeranosti a odradzujúceho účinku"*[216].

SDEÚ opakovane potvrdil, že vnútroštátne právne predpisy nie sú úplne slobodné, pokiaľ ide o určenie sankcií.

Príklad: SDEÚ vo veci *Von Colson a Kamann/Land Nordrhein-Westfalen*[217], poukázal na skutočnosť, že všetky členské štáty, ktorým je smernica určená, sú povinné prijať v rámci svojich vnútroštátnych právnych systémov všetky nevyhnutné opatrenia na zaistenie úplnej účinnosti smernice v súlade so stanovenými cieľmi. Súdny dvor potvrdil, že aj keď si členské štáty môžu vybrať spôsoby a prostriedky zabezpečenia vykonávania smernice, táto sloboda neovplyvňuje záväzok, ktorý im bol uložený. Predovšetkým musí existovať účinný právny prostriedok nápravy umožňujúci vykonávať a presadzovať príslušné právo v jeho úplnom podstatnom rozsahu. V záujme dosiahnutia skutočnej a účinnej ochrany musia právne prostriedky nápravy viesť k trestným konaniam alebo konaniam vo veci náhrady škody a následným sankciám s odradzujúcim účinkom.

Pokiaľ ide o sankcie za porušenia právnych predpisov EÚ inštitúciami alebo orgánmi EÚ, z dôvodu osobitného rozsahu pôsobnosti nariadenia o ochrane údajov inštitúciami EÚ sa predpokladajú len sankcie v podobe disciplinárnych opatrení. Podľa článku 49 uvedeného nariadenia „za každé nedodržanie povinností podľa tohto nariadenia, či už úmyselné alebo z nedbanlivosti, podlieha úradník alebo iný zamestnanec Európskych spoločenstiev disciplinárnemu konaniu […]".

216 FRA (2012), *stanovisko Agentúry Európskej únie pre základné práva k navrhovanému reformnému balíku týkajúcemu sa ochrany údajov*, 2/2012, Viedeň, 1. októbra 2012, s. 27.

217 SDEÚ, C-14/83, *Sabine von Kolson a Elisabeth Kamann/Land Nordrhein-Westfalen, 10. apríla 1984*.

6 Cezhraničné toky údajov

EÚ	Zahrnuté otázky	Rada Európy
Cezhraničné toky údajov		
Smernica o ochrane údajov, článok 25 ods. 1 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003	Vymedzenie pojmu	Dohovor č. 108, dodatkový protokol, článok 2 ods. 1
Voľný tok údajov		
Smernica o ochrane údajov, článok 1 ods. 2	Medzi členskými štátmi EÚ	
	Medzi zmluvnými stranami dohovoru č. 108	Dohovor č. 108, článok 12 ods. 2
Smernica o ochrane údajov, článok 25	Do tretích krajín s primeranou úrovňou ochrany údajov	Dohovor č. 108, dodatkový protokol, článok 2 ods. 1
Smernica o ochrane údajov, článok 26 ods. 1	Do tretích krajín v osobitných prípadoch	Dohovor č. 108, dodatkový protokol, článok 2 ods. 2 písm. a)
Obmedzený tok údajov do tretích krajín		
Smernica o ochrane údajov, článok 26 ods. 2 Smernica o ochrane údajov, článok 26 ods. 4	Zmluvné doložky	Dohovor č. 108, dodatkový protokol, článok 2 ods. 2 písm. b) Usmernenie o príprave zmluvných opatrení

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov, článok 26 ods. 2	Záväzné vnútropodnikové pravidlá	
Príklady: Dohoda medzi EÚ a USA o osobných záznamoch o cestujúcich (PNR) Dohoda medzi EÚ a USA o systéme SWIFT	Zvláštne medzinárodné dohody	

V smernici o ochrane údajov sa zaručuje voľný tok údajov nielen medzi členskými štátmi, ale obsahuje aj ustanovenia o požiadavkách na prenos osobných údajov do tretích krajín mimo EÚ. Aj Rada Európy si uvedomila význam vykonávacích pravidiel pre cezhraničné toky údajov do tretích krajín a v roku 2001 prijala dodatkový protokol k dohovoru č. 108. V protokole sa zaoberá hlavnými regulačnými vlastnosťami cezhraničných tokov údajov zo zmluvných strán dohovoru a členských štátov EÚ.

6.1. Povaha cezhraničných tokov údajov

Hlavné body

- Cezhraničný tok údajov je prenos osobných údajov k príjemcovi, na ktorého sa vzťahuje zahraničná jurisdikcia.

V článku 2 ods. 1 dodatkového protokolu k dohovoru č. 108 sa opisuje cezhraničný tok údajov ako prenos osobných údajov k príjemcovi, na ktorého sa vzťahuje zahraničná jurisdikcia. V článku 25 ods. 1 smernice o ochrane údajov sa upravuje „prenos osobných údajov, ktoré sa spracovávajú alebo sú určené na spracovanie po prenose [...]“. Tento prenos údajov je povolený len podľa pravidiel stanovených v článku 2 dodatkového protokolu k dohovoru č. 108 a v prípade členských štátov EÚ navyše v článkoch 25 a 26 smernice o ochrane údajov.

Príklad: SDEÚ vo veci *Bodil Lindqvist*[218] 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 podmien-

218 SDEÚ, C-101/01, *Bodil Lindqvist*, 6. novembra 2003, body 27, 68 a 69.

kach a o ich záľubách, predstavuje „úplne alebo čiastočne automatizované spracovanie osobných údajov“ v zmysle článku 3 ods. 1 smernice 95/46“.

Súdny dvor potom poukázal na to, že v smernici sa takisto stanovujú osobitné pravidlá, ktorých cieľom je umožniť členským štátom, aby monitorovali prenos osobných údajov do tretích krajín.

Vzhľadom na stav rozvoja internetu v čase vypracovania smernice, ako aj vzhľadom na to, že smernica neobsahuje kritériá uplatniteľné na použitie internetu „sa nemožno domnievať, že by zákonodarca Spoločenstva mal v úmysle do budúcnosti zahrnúť pod pojem „prenos údajov do tretích krajín“ aj uloženie údajov na internetovú stránku [...], a to aj napriek tomu, že sa tieto údaje takto sprístupnili osobám z tretích krajín, ktoré mali technické prostriedky na získanie prístupu k týmto údajom“.

Keby sa smernica mala „vykladať v tom zmysle, že k „prenosu údajov do tretej krajiny“ dochádza vždy, keď sa osobné údaje vložia na internetovú stránku, potom by tento prenos bol nevyhnutne prenosom uskutočneným do všetkých tretích krajín, kde existujú potrebné technické prostriedky na prístup na internet. Osobitný režim upravený v [smernici] by sa tak v prípade operácií vykonaných na internete nevyhnutne stal všeobecne platným režimom. Akonáhle by Komisia [...] zistila, že čo len jedna tretia krajina nezabezpečuje primeranú úroveň ochrany, členské štáty by boli povinné zabrániť akémukoľvek uvádzaniu osobných údajov na internet.“

Zásada, podľa ktorej uverejnenie (osobných) údajov samo osebe nemožno pokladať za cezhraničný tok údajov, sa týka aj online verejných registrov alebo masmédií, napríklad (elektronických) novín a televízie. Pojem „cezhraničného toku údajov“ zahŕňa len komunikáciu, ktorá je zameraná na konkrétnych príjemcov.

6.2. Voľné toky údajov medzi členskými štátmi alebo medzi zmluvnými stranami

Hlavné body

- Prenos osobných údajov do iného členského štátu Európskeho hospodárskeho priestoru alebo do štátu, ktorý je zmluvnou stranou dohovoru č. 108, nesmie byť ničím obmedzený.

V rámci právnych predpisov Rady Európy musí podľa článku 12 ods. 2 dohovoru č. 108 existovať voľný tok osobných údajov medzi stranami dohovoru. Vnútroštátnymi právnymi predpismi sa nesmie obmedzovať export osobných údajov do zmluvných strán, okrem prípadov, keď:

- si to vyžaduje osobitná povaha údajov[219] alebo
- obmedzenie je nevyhnutné s cieľom predísť obchádzaniu vnútroštátnych právnych ustanovení o cezhraničnom toku údajov do tretích krajín[220].

Podľa právnych predpisov EÚ sú obmedzenia alebo zákazy voľného toku údajov medzi členskými štátmi z dôvodu ochrany údajov zakázané, a to článkom 1 ods. 2 smernice o ochrane údajov. Oblasť voľného toku údajov sa rozšírila Dohodou o európskom hospodárskom priestore (EHP)[221], ktorej prostredníctvom 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 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 USA, slovinský vývozca údajov by sa musel podrobiť konaniu stanovenému v slovinských právnych predpisoch o cezhraničnom toku údajov do tretích krajín bez primeranej ochrany údajov, s výnimkou situácie, keď spoločnosť dodržiava zásady bezpečného prístavu, čo je dobrovoľný kódex správania pri poskytovaní primeranej úrovne ochrany údajov (pozri oddiel 6.3.1).

Ustanovenia smernice o ochrane údajov sa však nevzťahujú na cezhraničné toky údajov do členských štátov EHP na účely, ktoré sú mimo rozsahu pôsobnosti vnútorného trhu, napríklad pri vyšetrovaní trestných činov, a teda sa ich netýka zásada voľného toku údajov. Pokiaľ ide o právne predpisy Rady Európy,

219 Dohovor č. 108, článok 12 ods. 3 písm. a).

220 Tamtiež, článok 12 ods. 3 písm. b).

221 Rozhodnutie Rady a Komisie z 13. decembra 1993 o uzatvorení 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.

všetky oblasti sú zahrnuté do rozsahu pôsobnosti dohovoru č. 108 a dodatkového protokolu k dohovoru č. 108, aj keď zmluvné strany majú právo na výnimky. Všetci členovia EHP sú takisto zmluvnými stranami dohovoru č. 108.

6.3. Voľné toky údajov do tretích krajín

Hlavné body

- Prenos osobných údajov do tretích krajín nie je obmedzený vnútroštátnymi právnymi predpismi o ochrane údajov, ak:
  - je zaručená primeranosť ochrany údajov u príjemcu alebo
  - je to nevyhnutné v špecifickom záujme dotknutej osoby alebo v legitímnych prevyšujúcich záujmoch iných, predovšetkým v dôležitých verejných záujmoch.
- Primeranosť ochrany záujmov v tretej krajine znamená, že sa v rámci vnútroštátnych právnych predpisov danej krajiny účinne uplatňujú hlavné zásady ochrany údajov.
- Podľa právnych predpisov EÚ posudzuje primeranosť ochrany údajov v tretej krajine Európska komisia. V právnych predpisoch Rady Európy sa úprava spôsobu posúdenia primeranosti ponecháva na vnútroštátnych právnych predpisoch.

6.3.1. Voľný tok údajov z dôvodu primeranej ochrany

Právne predpisy Rady Európy umožňujú, aby sa vo vnútroštátnych právnych predpisoch povolil voľný tok údajov do štátov, ktoré nie sú zmluvnými stranami v prípade, že príjemca zabezpečí primeranú úroveň ochrany pre zamýšľaný prenos údajov[222]. Spôsob posúdenia úrovne ochrany v zahraničí, ako aj subjekt, ktorý posúdenie vykoná, sa určuje vnútroštátnymi právnymi predpismi.

Podľa právnych predpisov EÚ je voľný tok údajov do tretích krajín s primeranou úrovňou ochrany stanovený v článku 25 ods. 1 smernice o ochrane údajov. Požiadavka primeranosti na rozdiel od požiadavky rovnocennosti umožňuje akceptovať rôzne spôsoby vykonávania ochrany údajov. Podľa článku 25 ods. 6 smernice je Európska komisia oprávnená posúdiť úroveň ochrany v zahraničí prostredníctvom

222 Dohovor č. 108, dodatkový protokol, článok 2 ods. 1.

zistení o primeranosti a konzultovať toto posúdenie s pracovnou skupinou zriadenou podľa článku 29, ktorá významne prispela k výkladu článkov 25 a 26[223].

Zistenia Európskej komisie o primeranosti sú záväzné. Ak Európska komisia uverejní zistenie o primeranosti pre určitú krajinu v *Úradnom vestníku Európskej únie*, všetky členské štáty EHP a ich orgány sú povinné toto rozhodnutie rešpektovať, v tom zmysle, že tok údajov do príslušnej krajiny je možný bez kontroly alebo udelenia licencie zo strany vnútroštátnych orgánov[224].

Európska komisia môže posúdiť časti právneho systému príslušnej krajiny alebo sa zameria na určité témy. Komisia vydala zistenie o primeranosti napríklad výlučne vo veci kanadskej súkromnej obchodnej legislatívy[225]. Niekoľko zistení o primeranosti sa týka prenosov založených na dohodách medzi EÚ a zahraničnými štátmi. Tieto rozhodnutia sa týkajú výlučne jedného typu prenosu údajov, napríklad prenosu záznamov mien cestujúcich leteckými spoločnosťami zahraničným pohraničným orgánom pri letoch leteckých spoločností z EÚ do určitých zámorských destinácií (pozri oddiel 6.4.3). Najnovšou praxou prenosu údajov založenou na osobitných dohodách medzi EÚ a tretími krajinami sa vo všeobecnosti odstraňuje potreba zistení o primeranosti, keďže sa v rámci nej predpokladá, že primeraná úroveň ochrany údajov je zaistená samotnou dohodou[226].

Jedno z najdôležitejších rozhodnutí týkajúcich sa primeranosti sa v skutočnosti netýka súboru právnych ustanovení[227]. Ide skôr o pravidlá podobné kódexu sprá-

223 Pozri napríklad pracovná skupina zriadená podľa článku 29 (2003), *pracovný dokument o prenose osobných údajov do tretích krajín, ktorým sa uplatňuje článok 26 ods. 2 smernice EÚ o ochrane údajov na záväzné firemné pravidlá pri medzinárodnom prenose údajov*, WP 74, Brusel, 3. júna 2003, a 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.

224 Nepretržite aktualizovaný zoznam krajín, ktorým bolo priznané zistenie o primeranosti, nájdete na domovskej stránke Európskej komisie, Generálne riaditeľstvo pre spravodlivosť, na adrese: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Európska komisia (2002), Rozhodnutie 2002/2/ES 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.

226 Napríklad Dohoda medzi Spojenými štátmi americkými a Európskou úniou o využívaní osobných záznamov o cestujúcich a ich postupovaní Ministerstvu vnútornej bezpečnosti Spojených štátov amerických (Ú v. EÚ L 215, 2012, s. 5–14) alebo Dohoda medzi Európskou úniou a Spojenými štátmi americkými o spracovaní a zasielaní údajov obsiahnutých vo finančných správach z Európskej únie do Spojených štátov na účely Programu na sledovanie financovania terorizmu, Ú. v. EÚ L 8, 2010, s. 11–16.

227 Európska komisia (2000), 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, 2000.

vania, ktoré sú známe ako zásady bezpečného prístavu. Tieto zásady vypracovala EÚ spoločne s USA pre obchodné spoločnosti v USA. Členstvo v bezpečnom prístave sa zakladá na dobrovoľnom záväzku prijatom na Ministerstve obchodu USA a zdokumentovanom v zozname, ktorý ministerstvo uverejňuje. Keďže jednou z dôležitých zložiek primeranosti je účinnosť vykonávania ochrany údajov, dohodou o bezpečnom prístave sa zabezpečuje určitá miera štátneho dohľadu: k bezpečnému prístavu sa môžu pripojiť len tie spoločnosti, na ktoré sa vzťahuje dohľad Federálnej obchodnej komisie USA.

6.3.2. Voľný tok údajov v osobitných prípadoch

V rámci právnych predpisov Rady Európy sa článkom 2 ods. 2 dodatkového protokolu k dohovoru č. 108 umožňuje prenos osobných údajov do tretích krajín, v ktorých sa neuplatňuje primeraná ochrana údajov, pokiaľ je takýto prenos predpísaný vnútroštátnymi právnymi predpismi a je nevyhnutný z dôvodu:

- špecifických záujmov dotknutých osôb alebo
- legitímnych prednostných záujmov iných, najmä dôležitých verejných záujmov.

V rámci právnych predpisov EÚ sú v článku 26 ods. 1 smernice o ochrane údajov uvedené ustanovenia, ktoré sa podobajú ustanoveniam dodatkového protokolu k dohovoru č. 108.

Podľa smernice môžu záujmy dotknutých osôb oprávňovať voľný tok údajov do tretích krajín, ak:

- bol poskytnutý jednoznačný súhlas dotknutej osoby s vývozom údajov alebo
- dotknutá osoba nadväzuje zmluvný vzťah (alebo sa pripravuje na jeho nadviazanie), ktorý si jasne vyžaduje presun údajov k príjemcom v zahraničí, alebo
- bola uzatvorená zmluva medzi prevádzkovateľom a treťou stranou v záujmoch dotknutej osoby, alebo
- prenos je nevyhnutne potrebný na ochranu životných záujmov dotknutej osoby
- v prípade prenosu údajov z verejných registrov – to je prípad prednostných záujmov širokej verejnosti s cieľom získať možnosť sprístupnenia informácií uchovávaných vo verejných registroch.

Cezhraničný tok údajov môže byť oprávnený legitímnymi záujmami iných[228]:

- z dôvodu dôležitého verejného záujmu iného ako sú otázky vnútroštátnej alebo verenej bezpečnosti, keďže týmito otázkami sa v smernici o ochrane údajov nezaoberá alebo

- na účely stanovenia, vykonania alebo obhajoby právnych nárokov.

Uvedené príklady treba chápať ako výnimky z pravidla, podľa ktorého si voľný prenos údajov do iných krajín vyžaduje primeranú úroveň ochrany údajov v prijímajúcej krajine. Výnimky sa vždy musia vykladať reštriktívne. To opakovane zdôraznila pracovná skupina zriadená podľa článku 29 v súvislosti s článkom 26 ods. 1 smernice o ochrane údajov, predovšetkým vtedy, keď je základom prenosu údajov údajný súhlas[229]. Pracovná skupina zriadená podľa článku 29 dospela k záveru, že všeobecné pravidlá právnej váhy súhlasu sa vzťahujú aj na článok 26 ods. 1 smernice. Ak napríklad v kontexte pracovných vzťahov nie je jasné, či bol súhlas poskytnutý zamestnancom skutočne slobodný, prenosy údajov nemôžu byť založené na článku 26 ods. 1 písm. a) smernice. V týchto prípadoch sa bude uplatňovať článok 26 ods. 2, v ktorom sa vyžaduje, aby vnútroštátne orgány pre ochranu údajov vydali povolenie na prenosy údajov.

6.4. Obmedzené toky údajov do tretích krajín

Hlavné body

- Pred exportom údajov do tretích krajín, ktoré nezaisťujú primeranú úroveň ochrany údajov, môže prevádzkovateľ podrobiť zamýšľaný tok údajov prešetreniu zo strany dozorného orgánu.
- Prevádzkovateľ, ktorý chce exportovať údaje, musí počas vyšetrovania preukázať dve skutočnosti:
  - že existuje právny základ pre prenos údajov príjemcovi;

228 Smernica o ochrane údajov, článok 26 ods. 1 písm. d).

229 Pozri predovšetkým: 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.

  - že boli prijaté opatrenia, ktorými sa zabezpečí primeraná ochrana údajov u príjemcu.
- Opatrenia na zaistenie primeranej ochrany údajov u príjemcu môžu zahŕňať:
  - zmluvné dojednania medzi prevádzkovateľom exportujúcim údaje a zahraničným príjemcom údajov alebo
  - záväzné vnútropodnikové pravidlá, ktoré sa zvyčajne uplatňujú na prenosy údajov v rámci nadnárodných skupín spoločností.
- Prenosy údajov zahraničným orgánom môžu byť upravené tiež zvláštnou medzinárodnou dohodou.

V smernici o ochrane údajov a v dodatkovom protokole k dohovoru č. 108 sa povoľuje, aby sa vo vnútroštátnych právnych predpisoch ustanovili režimy pre zahraničné toky údajov do tretích krajín, ktoré nezaisťujú primeranú úroveň ochrany údajov, pokiaľ prevádzkovateľ prijal osobitné opatrenia na zaistenie záruk primeranej ochrany údajov u príjemcu a pokiaľ túto skutočnosť môže dokázať príslušnému orgánu. Táto požiadavka je síce výslovne uvedená len v dodatkovom protokole k dohovoru č. 108, považuje sa však za štandardný postup aj podľa smernice o ochrane údajov.

6.4.1. Zmluvné doložky

V oboch právnych poriadkoch – **Rady Európy** 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 príjemcu.

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 údajov[230]. Keďže rozhodnutia Komisie sú záväzné v celom rozsahu v členských štátoch, vnútroštátne orgány poverené dozorom nad cezhraničnými tokmi údajov musia vo svojich postupoch uznávať tieto zmluvné doložky[231]. 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.

230 Smernica o ochrane údajov, článok 26 ods. 4.

231 ZFEÚ, článok 288.

Existencia štandardných zmluvných opatrení v právnom rámci EÚ nebráni prevádzkovateľom, aby sformulovali iné zmluvné doložky *ad hoc*. Mali by však zaisťovať rovnakú úroveň ochrany, akú poskytujú štandardné zmluvné doložky. 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 opatrení pre prenosy medzi prevádzkovateľmi, z ktorých si prevádzkovateľ exportujúci údaje môže vybrať[232]. V prípade prenosov od prevádzkovateľa k sprostredkovateľovi existuje len jeden súbor štandardných zmluvných opatrení[233].

Pokiaľ ide o **právne predpisy Rady Európy**, poradný výbor pre dohovor č. 108 vypracoval usmernenie o príprave zmluvných opatrení[234].

6.4.2. Záväzné vnútropodnikové pravidlá

Viacstranné záväzné vnútropodnikové pravidlá veľmi často zahŕňajú niekoľko európskych orgánov pre ochranu údajov[235]. V záujme schválenia záväzných firemných

232 Súbor I je uvedený v prílohe k dokumentu Európska komisia (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 uvedený v prílohe k dokumentu Európska komisia (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.

233 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.

234 Rada Európy, poradný výbor pre dohovor č. 108 (2002), Usmernenia o príprave zmluvných opatrení upravujúcich ochranu údajov pri prenose osobných údajov tretím stranám, ktoré nie sú viazané primeranou úrovňou ochrany údajov.

235 Obsah a štruktúra príslušných záväzných firemných pravidiel sú vysvetlené v dokumente pracovnej skupiny zriadenej podľa článku 29 (2008), *pracovný dokument, ktorým sa stanovuje rámec štruktúry záväzných firemných opatrení*, WP 154, Brusel, 24. júna 2008 a dokumente pracovnej skupiny zriadenej podľa článku 29 (2008), *pracovný dokument, ktorým sa stanovuje tabuľka so zložkami a zásadami, ktoré majú byť súčasťou záväzných firemných pravidiel,* WP 153, Brusel, 24. júna 2008.

pravidiel je nutné odoslať návrh pravidiel spolu so štandardnými formulármi žiadosti hlavnému orgánu[236]. Hlavný orgán je možné určiť podľa štandardizovaného formulára žiadosti. Hlavný orgán následne informuje všetky dozorné orgány v členských štátoch EHP, v ktorých sídlia pobočky skupiny, hoci ich účasť v hodnotení záväzných firemných pravidiel je dobrovoľná. Všetky orgány pre ochranu údajov by mali zahrnúť výsledok hodnotenia do svojich formálnych postupov udeľovania povolení, aj keď toto pravidlo nie je záväzné.

6.4.3. Zvláštne medzinárodné dohody

EÚ uzatvorila zvláštne dohody týkajúce sa dvoch typov prenosu údajov:

Osobné záznamy o cestujúcich

Údaje v osobných záznamoch o cestujúcich (PNR) zbierajú letecké spoločnosti v rámci rezervácie letenky. Ide o meno, adresu, údaje o platobnej karte a číslo sedadla cestujúceho. Podľa právnych predpisov USA sú letecké spoločnosti povinné sprístupniť tieto údaje Ministerstvu vnútornej bezpečnosti pred odletom cestujúcich. Toto ustanovenie sa týka letov do a zo Spojených štátov.

Za účelom zabezpečenia primeranej ochrany osobných záznamov o cestujúcich (PNR) a v súlade s ustanoveniami smernice 95/46/ES, bol v roku 2004 ustanovený systém ochrany osobných záznamov o cestujúcich (PNR).[237] Tento systém odkazuje na primeranosť spracovania osobných údajov ministerstvom vnútornej bezpečnosti Spojených štátov (DHS). Po anulovaní systému ochrany osobných záznamov o cestujúcich (PNR) Súdnym dvorom[238] boli podpísané dve dohody s dvoma cieľmi: po prvé, poskytnúť právny základ pre zverejnenie údajov v osobných záznamoch o cestujúcich (PNR) zahraničným orgánom Spojených štátov a po druhé, zaistiť primeranú ochranu údajov v prijímajúcej krajine.

---

236 Pracovná skupina zriadená podľa článku 29 (2007), *stanovisko 1/2007 k pojmu osobných údajov*, WP 133, 20. júna 2007, s. 22.

237 Rozhodnutie Rady 2004/496/ES zo 17. mája 2004 o uzavretí dohody medzi Európskym spoločenstvom a Spojenými štátmi americkými o spracovaní a postúpení údajov PNR leteckými dopravcami Úradu pre colnú správu a ochranu hraníc, U. v. EU L 183, 2004. s. 83 a rozhodnutie Komisie 2004/535/ES zo 14. mája 2004 o adekvátnej ochrane osobných údajov uvedených v Zázname podľa mena cestujúceho o cestujúcich lietadlom odoslaných Úradu Spojených štátov na ochranu colného priestoru a hraníc, U. v. EU L 235, 2004, s. 11-22.

238 SDEU, Spojené veci C-317/04 a C-318-04 *Európsky parlament/Rada EÚ*, 30. Mája 2006, body 57, 58 a 59, kde súd rozhodol, že dohoda týkajúca sa prenosu rovnakých údajov ako aj rozhodnutie o primeranosti sú je vylúčené z pôsobnosti smernice.

Prvá dohoda o spoločnom využívaní a spravovaní údajov medzi krajinami EÚ a Spojenými štátmi americkými, podpísaná v roku 2012, obsahovala niekoľko chýb a bola nahradená v tom istom roku novou dohodou, ktorá zabezpečila väčšiu právnu istotu.[239] Nová dohoda je podstatne lepšia. Obmedzujú a vysvetľujú sa v nej účely, na ktoré sa informácie môžu použiť, napríklad závažné nadnárodné trestné činy a terorizmus a ustanovuje lehotu uchovávania údajov: po šiestich mesiacoch budú údaje zamaskované a anonymizované. V prípade zneužitia údajov má každý právo na správnu a súdnu nápravu v súlade s právnymi predpismi USA. Každý má tiež právo prístupu ku svojim údajom v osobnom zázname o cestujúcom (PNR) a právo úpravy ministerstvom vnútornej bezpečnosti vrátane možnosti vymazania nepresných informácií.

Dohoda, ktorá nadobudla účinnosť 1. júla 2012, bude účinná sedem rokov – do roku 2019.

Rada Európskej únie v decembri 2011 schválila uzatvorenie zaktualizovanej dohody medzi EÚ a Austráliou o spracovaní a prenose údajov v osobných záznamoch o cestujúcich (PNR)[240]. Dohoda medzi EÚ a Austráliou o údajoch v osobných záznamoch o cestujúcich (PNR) je ďalším krokom programu EÚ, ktorý zahŕňa celosvetové usmernenia o PNR[241], stanovenie systému osobných záznamov o cestujúcich (PNR) v EÚ[242] a uzatvorenie dohôd s tretími krajinami[243].

239 Rozhodnutie Rady 2012/472/EÚ z 26. apríla 2012 o uzavretí Dohody medzi Spojenými štátmi americkými a Európskou úniou o využívaní osobných záznamov o cestujúcich a ich postupovaní Ministerstvu vnútornej bezpečnosti Spojených štátov amerických, Ú. v. EÚ L 215/4, 2012. Text dohody je priložený k rozhodnutiu, Ú. v. EÚ L 215, 2012, s. 5–14.

240 Rozhodnutie Rady 2012/381/EÚ z 13. decembra 2011 o uzavretí Dohody medzi Európskou úniou a Austráliou o spracovaní a prenose údajov z osobného záznamu o cestujúcom (PNR) leteckými dopravcami Austrálskemu úradu pre colnú správu a ochranu hraníc, Ú. v. EÚ L 186/3, 2012. Text dohody, ktorý nahradil predošlú dohodu z roku 2008, je priložený k rozhodnutiu, Ú. v. EÚ L 186, 2012, s. 4–16.

241 Pozri predovšetkým oznámenie Komisie z 21. septembra 2010 o všeobecnom prístupe k prenosu osobných záznamov o cestujúcich do tretích krajín, KOM(2010) 0492 v konečnom znení, Brusel, 21. septembra 2010. Pozri tiež stanovisko č. 7/2010 k oznámeniu Európskej komisie o všeobecnom prístupe k prenosu osobných záznamov o cestujúcich do tretích krajín, WP 178, Brusel, 12. Novembra 2010.

242 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. V apríli 2011 Európsky parlament požiadal agentúru FRA o stanovisko k tomuto návrhu a jeho súladu s Chartou základných práv Európskej únie. Pozri: FRA (2011), *stanovisko 1/2011 – Záznam mena cestujúceho*, Viedeň, 14. júna 2011.

243 EÚ rokuje o uzatvorení novej dohody o osobných záznamoch o cestujúcich (PNR) s Kanadou, ktorá nahradí v súčanosti účinnú dohodu z roku 2006.

Údaje z finančných správ

Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT) so sídlom v Belgicku, ktorá je sprostredkovateľom väčšiny celosvetových prevodov peňazí z európskych bánk, prevádzkovala so „zrkadlovým" strediskom v Spojených štátoch amerických. Musela reagovať na žiadosť ministerstva financií USA o zverejnenie údajov na účely vyšetrovania terorizmu[244].

Z hľadiska EÚ neexistoval žiadny dostatočný právny dôvod na zverejnenie v podstate európskych údajov, ktoré boli v USA prístupné len preto, lebo tam sídlili servisné strediská na spracovanie 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 ochranu údajov[245].

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 údajov od spoločnosti SWIFT pod podmienkou, že žiadosť:

- čo najjasnejšie vymedzuje finančné údaje;
- jasne zdôvodňuje nevyhnutnosť údajov;
- je koncipovaná čo najužšie s cieľom minimalizovať objem požadovaných údajov;
- nepožaduje poskytnutie žiadnych údajov týkajúcich sa jednotnej oblasti platieb v eurách (SEPA).

244 V tejto súvislosti pozri dokument pracovnej skupiny zriadenej podľa článku 29 (2011), *stanovisko 14/2011 k otázkam ochrany údajov súvisiacich s predchádzaním praniu špinavých peňazí a financovaniu terorizmu*, WP 186, Brusel, 13. júna 2011; dokument pracovnej skupiny zriadenej podľa článku 29 (2006), *stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT)*, WP 128, Brusel, 22. novembra 2006; dokument belgickej komisia pre ochranu súkromia (Commission de la protection de la vie privée) (2008), Postup kontroly a odporúčania otvorené v súvislosti so spoločnosťou SWIFT scrl, rozhodnutie, 9. decembra 2008.

245 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. 5–14.

Kópia každej žiadosti ministerstva financií USA musí byť zaslaná Europolu a Europol musí overiť, či je v súlade so zásadami dohody o spoločnosti SWIFT.[246] 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 vyšetrujúci terorizmus alebo jeho financovanie. Finančné údaje nesmú byť prepojené so žiadnou inou databázou. Finančné údaje získané od spoločnosti sa odstránia 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.

Ministerstvo financií USA môže prenášať informácie z údajov od spoločnosti SWIFT konkrétnym orgánom presadzovania práva, verejnej bezpečnosti alebo boja proti terorizmu v USA alebo za ich hranicami 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, každé spoločné využívanie údajov s orgánmi tretej krajiny si vyžaduje predchádzajúci súhlas príslušných orgánov dotknutého členského štátu. Výnimky sú možné v prípade, že spoločné využívanie 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.

Dotknuté osoby majú právo na potvrdenie príslušného orgánu EÚ pre ochranu údajov o dodržaní práv na ochranu osobných údajov. Dotknuté osoby majú tiež právo úpravy, vymazania alebo blokovania svojich údajov zozbieraných a uložených ministerstvom financií USA podľa dohody SWIFT. Na práva prístupu dotknutých osôb sa môžu vzťahovať určité právne obmedzenia. V prípade zamietnutia prístupu musí byť dotknutá osoba písomne informovaná o zamietnutí a o práve na správnu alebo súdnu nápravu v USA.

Dohoda o spoločnosti SWIFT je účinná päť rokov do augusta 2015. Automaticky sa predlžuje o jeden rok, kým jedna zmluvná strana neoznámi druhej zmluvnej strane, a to v predstihu aspoň šesť mesiacov, že nemá v úmysle predĺžiť účinnosť dohody.

246 Spoločný dozorný orgán Europolu uskutočnil audit aktivít Europolu v tejto oblasti a výsledky tohto auditu sú dostupné na: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

7

Ochrana údajov v kontexte polície a trestného súdnictva

EÚ	Zahrnuté otázky	Rada Európy
	Vo všeobecnosti	Dohovor č. 108
	Polícia	Odporúčanie v oblasti polície
		ESĽP, *B. B./Francúzsko*, č. 5335/06, 17. decembra 2009
		ESĽP, *S. a Marper/Spojené kráľovstvo*, č. 30562/04 a 30566/04, 4. decembra 2008
		ESĽP, *Vetter/Francúzsko*, č.59842/00, 31. mája 2005
	Počítačová kriminalita	Dohovor o počítačovej kriminalite
Ochrana údajov v kontexte cezhraničnej spolupráce policajných a justičných orgánov		
Rámcové rozhodnutie o ochrane údajov	**Vo všeobecnosti**	Dohovor č. 108 Odporúčanie v oblasti polície
Prümské rozhodnutie	**Pre osobitné údaje: odtlačky prstov, DNA, výtržníctvo atď.**	Dohovor č. 108 Odporúčanie v oblasti polície
Rozhodnutie o Europole Rozhodnutie o Eurojuste Nariadenie o agentúre Frontex	**Osobitnými agentúrami**	Dohovor č. 108 Odporúčanie v oblasti policajných údajov

EÚ	Zahrnuté otázky	Rada Európy
Rozhodnutie Schengen II Nariadenie o vízovom informačnom systéme (VIS) Nariadenie o systéme Eurodac Rozhodnutie o colnom informačnom systéme (CIS)	Osobitnými spoločnými informačnými systémami	Dohovor č. 108 Odporúčanie v oblasti polície ESĽP, *Dalea/Francúzsko*, č. 964/07, 2. februára 2010

EÚ aj Rada Európy prijali osobitné právne nástroje v záujme vyváženia individuálnych záujmov v oblasti ochrany údajov a záujmov spoločnosti v oblasti zhromažďovania údajov na účely boja proti trestnej činnosti a zabezpečenia vnútroštátnej a verejnej bezpečnosti.

7.1. Právne predpisy Rady Európy týkajúce sa ochrany údajov vo veciach polície a trestného súdnictva

Hlavné body

- Dohovor č. 108 a odporúčanie Rady Európy v oblasti polície sa týkajú ochrany údajov vo všetkých oblastiach policajnej činnosti.
- Dohovor o počítačovej kriminalite (*Budapeštiansky dohovor*) je záväzný medzinárodný právny nástroj, ktorý sa zaoberá trestnou činnosťou zameranou na elektronické siete a páchanou ich prostredníctvom.

Na európskej úrovni dohovor č. 108 zahŕňa všetky oblasti spracovania osobných údajov a cieľom jeho ustanovení je všeobecná regulácia spracúvania osobných údajov. Z toho vyplýva, že dohovor č. 108 sa týka aj ochrany údajov v oblasti polície a trestného súdnictva, hoci zmluvné strany môžu obmedziť jeho uplatňovanie.

Právne úlohy orgánov polície a trestného súdnictva si často vyžadujú spracúvanie osobných údajov, ktoré môže mať pre dotknutých jednotlivcov vážne dôsledky. Odporúčaním v oblasti policajných údajov prijatým Radou Európy v roku 1987 sa

usmerňujú zmluvné strany, pokiaľ ide o spôsob vykonávania zásad dohovoru č. 108 v kontexte spracúvania osobných údajov policajnými orgánmi[247].

7.1.1. Odporúčanie v oblasti polície

ESĽP neustále zdôrazňuje, že uchovávanie osobných údajov políciou alebo orgánmi vnútroštátnej bezpečnosti predstavuje zasahovanie v zmysle článku 8 ods. 1 EDĽP. V mnohých rozsudkoch ESĽP sa rieši otázka opodstatnenosti takýchto zásahov[248].

Príklad: ESĽP vo veci *B. B./Francúzsko*[249] rozhodol, že zahrnutie osoby odsúdenej za sexuálny trestný čin do vnútroštátnej súdnej databázy patrí do rozsahu pôsobnosti článku 8 EDĽP. 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 EDĽP.

Príklad: Vo veci *S. a Marper/Spojené kráľovstvo*[250] 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 činu dokonca aj vtedy, keď bola neskôr zbavená obvinenia alebo prepustená. ESĽP 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 EDĽP.

Veľa ďalších rozsudkov ESĽP sa týka opodstatnenosti zasahovania do práva na ochranu údajov sledovaním.

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

248 Pozri napríklad ESĽP, *Leander/Švédsku*, č. 9248/81, 26. marca 1987; ESĽP, *M.M./Spojené kráľovstvo*, č. 24029/07, 13. novembra 2012; ESĽP, *M. K./Francúzsko*, č. 19522/09, 18. apríla 2013.

249 ESĽP, *B.B./Francúzsko*, č. 5335/06, 17. decembra 2009.

250 ESĽP, *S. a Marper/Spojené kráľovstvo*, č. 30562/04 a 30566/04, 4. decembra 2008, body 119 a 125.

Príklad: Vo veci *Allan/Spojené kráľovstvo*[251] orgány tajne nahrávali súkromné rozhovory väzňa s jeho priateľom v miestnosti vyhradenej pre návštevy a s ďalším obvineným vo väzenskej cele. ESĽP potvrdil, 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 štatutárny 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 EDĽP.

Príklad: Vo veci *Klass a iní/Nemecko*[252] sťažovatelia tvrdili, že niekoľko nemeckých legislatívnych aktov povoľujúcich tajné sledovanie elektronickej pošty, poštových zásielok a telekomunikácie porušuje článok 8 EDĽP, a to predovšetkým preto, lebo príslušná osoba nie je informovaná o opatreniach vyplývajúcich zo sledovania a nemá možnosť obrátiť sa na súd po skončení opatrení. ESĽP potvrdil, že hrozba sledovania je určite porušením slobody komunikácie medzi používateľmi poštových a telekomunikačných služieb. Zistil však aj to, že boli prijaté dostatočné záruky proti zneužitiu. Nemecké právne predpisy oprávnene považovali takéto opatrenia za nevyhnutné v demokratickej spoločnosti v záujme vnútroštátnej bezpečnosti a predchádzania neporiadku alebo trestnej činnosti. Súd dospel k záveru, že nedošlo k porušeniu článku 8 EDĽP.

Keďže spracúvanie údajov policajnými orgánmi môže mať významný vplyv na dotknuté osoby, je nutné prijať podrobné pravidlá ochrany údajov pri vedení databáz v tejto oblasti. Na riešenie tohto problému bolo určené odporúčanie Rady Európy v oblasti polície, ktoré poskytuje usmernenia o spôsobe zhromažďovania údajov pre policajnú činnosť, spôsobe uchovávania súborov s údajmi, 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. Rozoberá sa v ňom aj povinnosť zabezpečiť primeranú bezpečnosť osobných údajov.

Odporúčanie neobhajuje neobmedzený a nediferencovaný zber údajov policajnými orgánmi. Je v ňom obmedzený na mieru nevyhnutne potrebnú na predchádzanie skutočnému nebezpečenstvu alebo potlačovanie špecifických trestných činov. Každý dodatočný zber údajov by mal vychádzať z konkrétnych vnútroštátnych

251 ESĽP, *Allan/Spojené kráľovstvo*, č. 48539/99, 5. novembra 2002.

252 ESĽP, *Klass a iní/Nemecko*, č. 5029/71, 6. septembra 1978.

predpisov. Spracovanie citlivých údajov by sa malo obmedziť na mieru, ktorá je nevyhnutne potrebná v kontexte konkrétneho vyšetrovania.

Ak sa zbierajú osobné údaje bez vedomia dotknutej osoby, dotknutú osobu je nutné informovať o takomto zbere ihneď po tom, ako zverejnenie nebude brániť vyšetrovaniu. Zber údajov pomocou prostriedkov technického sledovania alebo iných automatizovaných prostriedkov by sa mal tiež zakladať na špecifických právnych ustanoveniach.

Príklad: Vo veci *Vetter/Francúzsko*[253] anonymný svedok obvinil sťažovateľa z vraždy. Keďže sťažovateľ pravidelne navštevoval domácnosť svojho priateľa, polícia tam so súhlasom vyšetrujúceho sudcu nainštalovala odpočúvacie zariadenie. Na základe zaznamenaných rozhovorov bol sťažovateľ uväznený a obžalovaný z vraždy. Sťažovateľ požiadal, aby nahrávka nebola prijatá ako prípustný dôkaz a argumentoval tým, že nebola umožnená právnymi predpismi. ESĽP musel rozhodnúť, či použitie odpočúvacieho zariadenia bolo alebo nebolo „v súlade správnymi predpismi". Odpočúvanie súkromných priestorov zjavne nebolo v súlade s článkami 100 a ďalšími Trestného poriadku, keďže uvedené ustanovenia sa týkali odpočúvania telefonických liniek. V článku 81 Trestného poriadku sa dostatočne jasne neuvádza rozsah ani spôsob voľnej úvahy orgánov pri povoľovaní monitorovania súkromných rozhovorov. Sťažovateľ teda nemal zaručený minimálny stupeň ochrany, na ktorý majú občania nárok v právnom štáte a demokratickej spoločnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

V odporúčaní sa dospieva k záveru, že pri uchovávaní osobných údajov sa musia jasne rozlišovať: administratívne údaje a policajné údaje, rôzne druhy dotknutých osôb, napríklad podozrivé osoby, odsúdené osoby, obete a svedkovia, ako aj údaje, ktoré treba považovať za reálne fakty, a tie, ktoré sa zakladajú na podozrení alebo domnienkach.

Pri policajných údajoch musí byť prísne obmedzený účel. To ovplyvňuje oznamovanie policajných údajov tretím stranám: prenos alebo oznámenie takýchto údajov v rámci policajného sektora by sa mali riadiť tým, či existuje alebo neexistuje legitímny záujem na spoločnom využívaní takýchto informácií. Prenos alebo oznámenie takýchto údajov mimo policajného sektora by sa mali povoliť len vtedy, ak

253 ESĽP, *Vetter/Francúzsko*, č.59842/00, 31. mája 2005.

existuje jasný právny záväzok alebo oprávnenie. Medzinárodný prenos alebo oznámenie 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.

Spracovanie údajov políciou musí podliehať nezávislému dozoru s cieľom zaistiť súlad s vnútroštátnymi predpismi na ochranu údajov. Dotknuté osoby musia mať všetky práva prístupu uvedené v dohovore č, 108. V prípade, že sú práva prístupu dotknutých osôb obmedzené podľa článku 9 dohovoru č. 108 v záujme efektívneho policajného vyšetrovania, dotknutá osoba musí mať podľa vnútroštátnych právnych predpisov právo na odvolanie k vnútroštátnemu dozornému orgánu pre ochranu údajov alebo inému nezávislému orgánu.

7.1.2. Budapeštiansky dohovor o počítačovej kriminalite

Keďže trestná činnosť stále častejšie používa a ovplyvňuje elektronické systémy na spracovanie údajov, sú potrebné nové trestnoprávne ustanovenia, ktoré budú na tento stav reagovať. Rada Európy preto prijala medzinárodný právny nástroj – dohovor o počítačovej kriminalite, taktiež známy ako Budapeštiansky dohovor, s cieľom riešiť problém trestnej činnosti páchanej proti elektronickým sieťam a ich prostredníctvom[254]. Dohovor je otvorený na pristúpenie aj štátom, ktoré nie sú členmi Rady Európy. Do polovice roku 2013 sa stali stranami dohovoru štyri štáty mimo Rady Európy – Austrália, Dominikánska republika, Japonsko a Spojené štáty americké a 12 ďalších nečlenov dohovor podpísalo alebo boli vyzvaní na pristúpenie.

Dohovor o počítačovej kriminalite je stále najvplyvnejšou medzinárodnou zmluvou, ktorá upravuje porušenie právnych predpisov týkajúcich sa internetu alebo iných informačných sietí. Vyžaduje sa v ňom, aby strany aktualizovali a harmonizovali svoje trestnoprávne ustanovenia proti hackerstvu a ďalším porušeniam bezpečnosti vrátane porušenia autorských práv, podvodov s využitím výpočtovej techniky, detskej pornografie a ďalších nezákonných počítačových činností. V dohovore sa takisto stanovujú procesné právomoci týkajúce sa vyhľadávania počítačových sietí a odpočúvania komunikácie v kontexte boja proti počítačovej kriminalite. Umožňuje aj

254 Rada Európy, Výbor ministrov (2001), Dohovor o počítačovej kriminalite, Súbor dohovorov Rady Európy č. 185, Budapešť, 23. novembra 2001, nadobudol účinnosť 1. júla 2004.

efektívnu medzinárodnú spoluprácu. Dodatkovým 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. V dohovore sa zmluvným stranám ukladá, aby pri jeho vykonávaní zohľadnili primeranú ochranu ľudských práv a slobôd vrátane práv zaručených EDĽP, napríklad práva na ochranu údajov[255].

7.2. Právne predpisy EÚ týkajúce sa ochrany údajov vo veciach polície a trestného súdnictva

Hlavné body

- Ochrana údajov v sektore polície a trestného súdnictva je na úrovni EÚ regulovaná len v kontexte cezhraničnej spolupráce policajných a súdnych orgánov.
- 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 oprávnenými policajnými a súdnymi orgánmi. Dôležitými príkladmi sú systémy Schengen II, vízový informačný systém (VIS) a Eurodac – centralizovaný systém obsahujúci údaje o odtlačkoch prstov štátnych príslušníkov tretích krajín žiadajúcich o azyl v niektorom z členských štátov EÚ.

Na oblasť polície a trestného súdnictva sa nevzťahuje smernica o ochrane údajov. Najdôležitejšie právne predpisy v tejto oblasti opisuje oddiel 7.2.1.

7.2.1. Rámcové rozhodnutie o ochrane údajov

Cieľom rámcového rozhodnutia Rady 2008/977/SVV o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach (*rámcové*

255 Tamtiež, článok 15 ods. 1.

rozhodnutie o ochrane údajov)[256] je poskytnutie ochrany osobných údajov fyzických osôb pri spracovaní ich osobných údajov na účely predchádzania trestným činom a ich vyšetrovania, zisťovania alebo stíhania alebo na účely vykonávania trestnoprávnych sankcií. Príslušné orgány pracujúce v oblasti polície a trestného súdnictva konajú v mene členských štátov alebo EÚ. Ide o agentúry a orgány EÚ, ako aj o orgány členských štátov[257]. Uplatniteľnosť rámcového rozhodnutia je obmedzená na zaistenie ochrany údajov pri cezhraničnej spolupráci medzi uvedenými orgánmi a nezasahuje do oblasti vnútroštátnej bezpečnosti.

Rámcové rozhodnutie o ochrane údajov sa do veľkej miery opiera o zásady a vymedzenia zahrnuté do dohovoru č. 108 a smernice o ochrane údajov.

Údaje smie používať len príslušný orgán a len na ten účel, na ktorý sa prenášajú alebo sprístupňujú. Prijímajúce členské štáty musia rešpektovať všetky obmedzenia týkajúce sa výmeny údajov, stanovené v právnych predpisoch členského štátu prenášajúceho údaje. Za určitých podmienok je však povolené použitie údajov prijímajúcim štátom na odlišný účel. Za protokolovanie a dokumentovanie prenosov osobitne zodpovedajú príslušné orgány s cieľom pomôcť pri ozrejmení povinností vyplývajúcich zo sťažností. Ďalší prenos údajov prijatých v rámci cezhraničnej spolupráce tretím stranám si vyžaduje súhlas členského štátu, z ktorého údaje pochádzajú, aj keď v naliehavých prípadoch existujú výnimky.

Príslušné orgány musia prijať nevyhnutné bezpečnostné opatrenia na ochranu osobných údajov pred nezákonnou formou spracúvania.

Každý členský štát musí zaistiť, aby jeden nezávislý vnútroštátny dozorný orgán alebo niekoľko dozorných orgánov zodpovedalo za poskytovanie poradenstva a monitorovanie uplatňovania ustanovení prijatých podľa rámcového rozhodnutia o ochrane údajov. Reagujú taktiež na sťažnosti rôznych osôb týkajúce sa ochrany ich práv a slobôd pri spracúvaní osobných údajov príslušnými orgánmi.

Dotknutá osoba má nárok na informácie o spracúvaní jej osobných údajov, právo prístupu a právo úpravy, vymazania alebo blokovania. Ak je vykonávanie týchto práv z presvedčivých dôvodov zamietnuté, dotknutá osoba musí mať právo na odvolanie k príslušnému vnútroštátnemu dozornému orgánu a/alebo súdu. Ak

256 Rada Európskej únie (2008), rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce (*rámcové rozhodnutie o ochrane údajov*), Ú. v. EÚ L 350, 2008.

257 Tamtiež, článok 2 písm. h).

osoba utrpí škodu z dôvodu porušenia vnútroštátnych právnych predpisov, ktorými sa vykonáva rámcové rozhodnutie o ochrane údajov, má nárok na odškodnenie od prevádzkovateľa[258]. Dotknuté osoby musia mať vo všeobecnosti prístup k opravnému prostriedku v prípade akéhokoľvek porušenia ich práv zaručených vnútroštátnymi právnymi predpismi, ktorými sa vykonáva rámcové rozhodnutie o ochrane údajov[259].

Európska komisia navrhla reformu, ktorú tvorí návrh všeobecného nariadenia o ochrane údajov[260] a smernica o všeobecnej ochrane údajov[261]. Nová smernica nahradí platné rámcové rozhodnutie o ochrane údajov a uplatnia sa v nej všeobecné zásady a pravidlá týkajúce sa policajnej a súdnej spolupráce v trestných veciach.

7.2.2. Špecifickejšie právne nástroje týkajúce sa ochrany údajov v rámci cezhraničnej spolupráce v oblasti polície a presadzovania práva

Výmena informácií uchovávaných členskými štátmi v špecifických oblastiach je okrem rámcového rozhodnutia o ochrane údajov regulovaná viacerými právnymi nástrojmi, napríklad rámcovým rozhodnutím Rady 2009/315/SVV o organizácii a obsahu výmeny informácií z registra trestov medzi členskými štátmi a rozhodnutím Rady upravujúcim spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov[262].

258 Tamtiež, článok 19.

259 Tamtiež, článok 20.

260 Európska komisia (2012), *návrh nariadenia Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov)*, KOM(2012) 11 v konečnom znení, Brusel, 25. januára 2012.

261 Európska komisia (2012), *návrh smernice Európskeho parlamentu a Rady 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 všeobecnej ochrane údajov)*, KOM(2012) 10 v konečnom znení, Brusel, 25. januára 2012.

262 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, 2009; Rada Európskej únie (2000), rozhodnutie Rady 2000/642/JHA zo 17. októbra 2000 upravujúce spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov, Ú. v. ES L 271, 2000.

Je dôležité, že cezhraničná spolupráca[263] medzi príslušnými orgánmi stále častejšie zahŕňa výmenu údajov o prisťahovalectve. Táto právna oblasť nepatrí k záležitostiam polície a trestného súdnictva, ale z viacerých hľadísk sa týka činnosti policajných a súdnych orgánov. Týka sa aj tovaru dovážaného do EÚ alebo vyvážaného z EÚ. Odstránením pohraničných kontrol v rámci EÚ 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.

Prümské rozhodnutie

Dôležitým príkladom inštitucionalizovanej cezhraničnej spolupráce formou výmeny údajov uchovávaných v členských štátoch je rozhodnutie Rady 2008/615/SVV z 23. júna 2008 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 zmluva[264]. Prümská zmluva bola medzinárodná dohoda o policajnej spolupráci, ktorú v roku 2005 podpísali Rakúsko, Belgicko, Francúzsko, Nemecko, Luxembursko, Holandsko a Španielsko[265].

Cieľom prümského rozhodnutia je pomôcť 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 rozsiahlymi udalosťami, ktoré majú cezhraničný rozmer;

263 Európska komisia (2012), oznámenie Komisie Európskemu parlamentu a Rade Posilnenie spolupráce v oblasti presadzovania práva v EÚ: európsky model výmeny informácií (EIXM), KOM(2012) 735 v konečnom znení, Brusel, 7. decembra 2012.

264 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.

265 Zmluva medzi Belgickým kráľovstvom, Spolkovou republikou Nemecko, Španielskym kráľovstvom, Francúzskou republikou, Luxemburským veľkovojvodstvom, Holandským kráľovstvom a Rakúskou republikou o zintenzívnení cezhraničnej spolupráce najmä v boji proti terorizmu, cezhraničnej trestnej činnosti a nelegálnej migrácii dostupná na adrese: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

- 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 a najnovšie aj rámcovým rozhodnutím o ochrane údajov. Príslušnými orgánmi dozerajúcimi na tieto toky údajov sú vnútroštátne dozorné orgány pre ochranu údajov.

7.2.3. Ochrana údajov v Europole a Eurojuste

Europol

Agentúra EÚ na presadzovanie práva – Europol – sídli v Haagu a v každom členskom štáte má národnú jednotku. Europol bol zriadený v roku 1998. Jeho súčasný právny štatút ako inštitúcie EÚ je založený na rozhodnutí Rady (*rozhodnutie o Europole*)[266]. Cieľom Europolu je pomáhať pri prevencii a vyšetrovaní organizovanej trestnej činnosti, terorizmu a ďalších foriem závažnej trestnej činnosti (ako sú uvedené v prílohe rozhodnutia o Europole), ktoré sa týkajú dvoch alebo viacerých členských štátov.

Europol zriadil v záujme dosiahnutia svojich cieľov európsky informačný systém, ktorý poskytuje členským štátom databázu na výmenu spravodajských informácií o trestnej činnosti a výmenu informácií prostredníctvom národných jednotiek. 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 jednotky 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.

266 Rada Európskej únie (2009), rozhodnutie Rady zo 6. apríla 2009 o zriadení Európskeho policajného úradu (Europol), Ú. v. EÚ L 121, 2009. Pozri taktiež návrh nariadenia Komisie, ktorým sa stanovuje právny rámec pre nový Europol, ktorý nadväzuje na a nahrádza Europol zriadený nariadením Rady 2009/371/SVV zo 6. apríla 2009, ktorým sa zriaďuje Európsky policajný úrad (Europol), a EPA zriadený rozhodnutím Rady 2005/681/SVV o zriadení Európskej policajnej akadémie (EPA), KOM(2013) 173 v konečnom znení.

Ak je to nevyhnutne potrebné pre plnenie úloh Europolu, Europol smie uchovávať, upravovať a používať údaje týkajúce sa trestných činov v analytických pracovných súboroch. Analytické pracovné súbory sú otvorené na účely spájania, spracúvania alebo používania údajov s cieľom pomáhať pri konkrétnych vyšetrovaniach trestnej činnosti vedených Europolom spolu s členskými štátmi EÚ.

Europol reaguje na súčasný vývoj a 1. januára 2013 zriadil Európske centrum boja proti počítačovej kriminalite[267]. Centrum slúži ako informačná križovatka EÚ v oblasti počítačovej kriminality. pomáha zrýchliť odozvu na trestnú činnosť on-line, vyvíja a zavádza digitálne forenzné funkcie a poskytuje osvedčené 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 životne dôležitú infraštruktúru a informačné systémy v EÚ.

Rozširuje sa režim ochrany údajov upravujúci činnosť Europolu. V článku 27 rozhodnutia o Europole sa uvádza, že platia zásady stanovené v dohovore č. 108 a v odporúčaní v oblasti policajných údajov, pokiaľ ide o spracovanie automatizovaných a neautomatizovaných údajov. Prenos údajov medzi Europolom a členskými štátmi sa tiež musí riadiť pravidlami uvedenými v rámcovom rozhodnutí o ochrane údajov.

V záujme zaistenia súladu s platnými právnymi predpismi o ochrane údajov a predovšetkým toho, aby pri spracovaní údajov nedochádzalo k porušovaniu práv jednotlivcov, je činnosť Europolu kontrolovaná a monitorovaná spoločným dozorným orgánom Europolu[268]. Každý jednotlivec má právo prístupu k osobným údajom, ktoré by o ňom Europol mohol uchovávať, ako aj právo požiadať o kontrolu, opravu alebo vymazanie týchto údajov. Ak nejaká osoba nie je spokojná s rozhodnutím Europolu týkajúcim sa vykonávania uvedených práv, môže sa odvolať k odvolaciemu výboru spoločného dozorného orgánu.

267 Pozri tiež: európsky dozorný úradník pre ochranu údajov (2012), *stanovisko dozorného úradníka pre ochranu údajov k oznámeniu Európskej Komisie Európskemu parlamentu a Rade o zriadení Európskeho centra boja proti počítačovej kriminalite*, Brusel, 29. júna 2012.

268 Rozhodnutie o Europole, článok 34.

Ak v dôsledku právnych alebo faktických chýb uchovávaných alebo spracovávaných Europolom dôjde ku vzniku škody, poškodená strana môže žiadať o nápravu na príslušnom súde členského štátu, v ktorom došlo k udalosti spôsobujúcej škodu[269]. Ak je škoda dôsledkom toho, že Europol nesplnil svoje právne povinnosti, odškodní členský štát.

Eurojust

Eurojust, zriadený v roku 2002, je orgán EÚ so sídlom v Haagu, ktorý podporuje súdnu spoluprácu pri vyšetrovaní a stíhaní závažnej trestnej činnosti týkajúcej sa minimálne dvoch členských štátov[270]. 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 sa vykonávajú vnútroštátnymi členmi. Každý členský štát vysiela do Eurojustu jedného sudcu alebo prokurátora, ktorého štatút je upravený vnútroštátnymi právnymi predpismi a ktorý má právomoci nevyhnutne potrebné pre plnenie úloh nutných na podporu a zlepšovanie súdnej spolupráce. Jednotliví členovia Eurojustu okrem toho konajú spoločne ako kolégium pri plnení osobitných úloh Eurojustu.

Eurojust môže spracovávať osobné údaje do tej miery, do akej je zo nutné pre dosiahnutie jeho cieľov. Spracovanie 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 spracovávať určité informácie týkajúce sa svedectiev

269 Tamtiež, článok 52.

270 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 44, 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*).

alebo obetí trestných činov v rozsahu svojej pôsobnosti[271]. Za výnimočných okolností môže v obmedzenom čase spracovávať 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.

Pokiaľ ide o ochranu údajov, Eurojust musí zaručiť úroveň ochrany aspoň rovnocennú zásadám 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 týkajúcimi sa ochrany údajov v Eurojuste[272].

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, úpravu, zablokovanie alebo vymazanie osobných údajov, môžu sa odvolať k spoločnému dozornému orgánu. 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.

7.2.4. 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 bolo zriadených niekoľko spoločných informačných systémov na úrovni EÚ, ktoré majú slúžiť ako platforma na výmenu údajov medzi príslušnými vnútroštátnymi a európskymi orgánmi na stanovené účely presadzovania práva vrátane imigračných a colných právnych predpisov. Niektoré z týchto systémov sa vyvinuli z viacstranných dohôd, ktoré boli následne doplnené právnymi nástrojmi a systémami EÚ, napríklad Schengenský informačný systém (SIS), vízový informačný systém (VIS), Eurodac, Eurosur a colný informačný systém (CIS).

271 Konsolidovaná verzia rozhodnutia Rady 2002/187/SVV zmeneného rozhodnutím Rady 2003/659/SVV a rozhodnutím Rady 2009/426/SVV, článok 15 ods. 2.

272 Ustanovenia vnútorných predpisov Eurojustu týkajúce sa spracovania a ochrany osobných údajov, Ú. v. EÚ C 68/01, 2005, 19. marca 2005, s. 1.

Za dlhodobé prevádzkové riadenie druhej generácie Schengenského informačného systému (SIS II), vízového informačného systému (VIS) a systému Eurodac zodpovedá Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (eu-LISA)[273] založená v roku 2012. Hlavnou úlohou agentúry je zaistiť efektívnu, bezpečnú a nepretržitú prevádzku systémov informačných technológií. Agentúra zodpovedá aj za prijatie nevyhnutných opatrení na zaistenie bezpečnosti systémov a údajov.

Schengenský informačný systém

V roku 1985 niekoľko členských štátov bývalých Európskych spoločenstiev 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 území[274]. Ako protiváha 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.

V dôsledku prístupu ďalších štátov k Schengenskej dohode bol schengenský systém napokon začlenený do právneho rámca EÚ prostredníctvom Amsterdamskej zmluvy[275]. 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 všetkým členským štátom EÚ a Islandu, Lichtenštajnsku, Nórsku a Švajčiarsku[276]. Prístup do systému SIS II má aj Europol a Eurojust.

Systém SIS II tvorí centrálny systém (C-SIS), vnútroštátne systémy (N-SIS) v jednotlivých členských štátoch a komunikačná infraštruktúra medzi centrálnym systémom

273 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.

274 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.

275 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.

276 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.

a vnútroštátnymi systémami. Systém C-SIS obsahuje určité údaje o osobách a predmetoch zadané členskými štátmi. Systém C-SIS používa vnútroštátna pohraničná kontrola, polícia, colníci, vízové a súdne orgány v celom schengenskom priestore. Jednotlivé členské štáty prevádzkujú kópie systému C-SIS, tzv. národné schengenské informačné systémy (N-SIS), ktoré sa nepretržite aktualizujú, čím sa aktualizuje aj systém C-SIS. Do systému N-SIS sa nahliada a systém vydá varovanie v prípade, že:

- osoba nemá právo vstúpiť na schengenské územie alebo na tomto území pobývať alebo
- po osobe alebo predmete pátrajú súdne orgány alebo orgány presadzovania práva, 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 vydania varovania musia národné schengenské informačné systémy prijať následné opatrenia.

Systém SIS II má nové funkcie, napríklad možnosť zadania: biometrických údajov (napríklad odtlačkov prstov a fotografií) alebo nových kategórií varovaní, ktoré sa týkajú napríklad odcudzených lodí, lietadiel, kontajnerov alebo platobných prostriedkov, rozšírené varovania týkajúce sa osôb a predmetov, kópie európskych zatýkacích rozkazov pre hľadané osoby, ktoré majú nastúpiť výkon trestu odňatia slobody alebo majú byť vydané.

Rozhodnutie Rady 2007/533/SVV o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (rozhodnutie o systéme SIS II) zahŕňa dohovor č. 108: „Osobné údaje spracúvané v rámci uplatňovania tohto rozhodnutia sú chránené v súlade s dohovorom Rady Európy z 28. januára 1981 o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov a jeho neskoršími zmenami a doplneniami.“[277] Ak vnútroštátne policajné orgány pri uplatňovaní rozhodnutia o SIS II používajú osobné údaje, v rámci vnútroštátnych právnych predpisov sa musia vykonávať ustanovenia dohovoru č. 108, ako aj odporúčania v oblasti policajných údajov.

277 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, článok 57.

Dozor nad vnútroštátnym systémom N-SIS vykonáva príslušný vnútroštátny dozorný orgán daného členského štátu. Predovšetkým musí kontrolovať kvalitu údajov, ktoré členské štáty zadávajú do systému C-SIS prostredníctvom systému N-SIS. Vnútroštátny dozorný orgán musí zaisťovať vykonanie auditu operácií spracovania údajov v rámci domáceho systému N-SIS, ktorý by sa mal uskutočniť každé štyri roky. Vnútroštátne dozorné orgány spolupracujú s európskym dozorným úradníkom pre ochranu údajov a zaisťujú koordinovaný dohľad nad systémom SIS, zatiaľ čo európsky dozorný úradník je zodpovedný za dohľad nad C-SIS. Z dôvodu transparentnosti sa každé dva roky zasiela spoločná správa o činnosti Európskemu parlamentu, Rade a agentúre eu-LISA.

Práva prístupu jednotlivcov týkajúce sa systému SIS II sa môžu vykonávať v každom členskom štáte, keďže každý systém N-SIS je presnou kópiou systému C-SIS.

Príklad: Vo veci *Dalea/Francúzsko*[278] bola zamietnutá žiadosť sťažovateľa o udelenie víza na návštevu Francúzska, keďže francúzske orgány do Schengenského informačného systému oznámili, 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. ESĽP dospel k záveru, že zanesenie mena sťažovateľa do Schengenského informačného systému bolo v súlade s právnymi predpismi a malo legitímny cieľ ochrany vnútroštátnej 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 pred svojvoľnými rozhodnutiami, zásah do jeho práva na rešpektovanie súkromného života bol primeraný. Sťažnosť sťažovateľa podľa článku 8 bola teda vyhlásená za neprípustnú.

Vízový informačný systém

Vízový informačný systém (VIS), ktorý prevádzkuje tiež agentúra eu-LISA, vznikol s cieľom pomôcť pri vykonávaní spoločnej vízovej politiky EÚ[279]. Systém VIS umožňuje výmenu údajov o vízach medzi schengenskými štátmi prostredníctvom

278 ESĽP, *Dalea/Francúzsko*, č. 964/07, 2. februára 2010.

279 Rada Európskej únie (2004), rozhodnutie Rady 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.

systému, ktorý spája veľvyslanectvá schengenských štátov v krajinách, ktoré nie sú členskými štátmi EÚ, s hraničnými priechodmi na vonkajších hraniciach všetkých schengenských štátov. V systéme VIS sa spracúvajú údaje týkajúce sa žiadostí o krátkodobé víza na účely návštevy alebo tranzitu cez schengenský priestor. Systém VIS umožňuje pohraničným orgánom, aby na základe biometrických údajov overili, či osoba, ktorá predkladá vízum, je alebo nie je jeho oprávneným držiteľom a aby identifikovali osoby bez dokladov alebo s podvodnými dokladmi.

Podľa nariadenia 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 v systéme VIS zaznamenávajú len údaje o žiadateľovi a jeho vízach, fotografie, odtlačky prstov, súvislosti s ostatnými žiadosťami a spisy žiadostí osôb, ktoré žiadateľa sprevádzajú[280]. Prístup do systému 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 sprístupnenie údajov zadaných do systému VIS požiadať príslušné vnútroštátne policajné orgány a Europol na účely prevencie, zisťovania a vyšetrovania teroristických a trestných činov[281].

Eurodac

Názov Eurodac odkazuje na daktylogramy, teda odtlačky prstov. Ide o centralizovaný systém obsahujúci údaje o odtlačkoch prstov štátnych príslušníkov tretích krajín, ktorí žiadajú o azyl v niektorom z členských štátov EÚ[282]. Systém funguje od januára 2003 a jeho účelom je pomôcť určiť konkrétny členský štát, ktorý by mal zodpovedať za vyšetrenie danej žiadosti o azyl podľa nariadenia Rady (ES) č. 343/2003

280 Článok 5 nariadenia 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.

281 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.

282 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 (*nariadenia o systéme Eurodac*), Ú. v. ES L 62, 2002.

z 18. februára 2003 ustanovujúceho kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o azyl podanej štátnym príslušníkom tretej krajiny v jednom z členských štátov (*Dublin II*)[283]. Osobné údaje v systéme Eurodac sa smú používať len na účely pomoci pri riešení žiadosti v rámci nariadenia Dublin II. Každé použitie na iný účel je postihnuteľné.

Systém Eurodac tvorí centrálna jednotka, prevádzkovaná agentúrou eu-LISA, určená na uchovávanie a porovnávanie odtlačkov prstov, a systém elektronického prenosu údajov medzi členskými štátmi a centrálnou databázou. Členské štáty odoberú a prenesú odtlačky prstov každého štátneho príslušníka krajiny, ktorá nie je členom EÚ, a každej osoby bez štátnej príslušnosti vo veku aspoň 14 rokov, ktorá požiada o azyl na ich území alebo ktorá bola zadržaná pri nelegálnom prechode ich vonkajších hraníc. Členské štáty môžu tiež odobrať a preniesť odtlačky prstov štátneho príslušníka krajiny, ktorá nie je členom EÚ, a každej osoby bez štátnej príslušnosti, u ktorej sa zistí, že pobýva na ich území bez povolenia.

Údaje o odtlačkoch prstov sa uchovávajú v databáze systému Eurodac len v pseudonymizovanej podobe. V prípade zhody je pseudonym spoločne s názvom prvého členského štátu, ktorý preniesol údaje o odtlačkoch prstov, oznámený druhému členskému štátu. Druhý členský štát sa potom obráti na prvý členský štát, keďže podľa nariadenia Dublin II je prvý členský štát zodpovedný za spracovanie žiadosti o azyl.

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 dva roky. Tieto údaje musia byť vymazané bezprostredne po tom, ako bude dotknutej osobe udelené povolenie na pobyt, ako dotknutá osoba opustí územie EÚ alebo získa občianstvo niektorého členského štátu.

Systém Eurodac využívajú okrem členských štátov EÚ aj Island, Nórsko, Lichtenštajnsko a Švajčiarsko, a to na základe medzinárodných dohôd.

283 Nariadenie Rady (ES) č. 343/2003 z 18. februára 2003 ustanovujúce kritériá a mechanizmy na určenie členského štátu zodpovedného za posúdenie žiadosti o azyl podanej štátnym príslušníkom tretej krajiny v jednom z členských štátov (*Dublin II*), Ú. v. EÚ L 50, 2003.

Eurosur

Cieľom Európskeho systému hraničného dozoru (*Eurosur*)[284] je rozšíriť kontrolu vonkajších hraníc schengenského priestoru prostredníctvom zisťovania, prevencie a boja proti nelegálnemu prisťahovalectvu a cezhraničnej trestnej činnosti. Tento systém súži na rozšírenie výmeny informácií a operačnej spolupráce medzi vnútroštátnymi koordinačnými strediskami a agentúrou Frontex, čo je agentúra EÚ zodpovedná za prípravu a realizáciu novej koncepcie integrovaného riadenia hraníc[285]. Medzi jej všeobecné ciele patrí:

- znížiť počet nezistených nelegálnych prisťahovalcov, ktorí vstúpia na územie EÚ;
- znížiť počet úmrtí nelegálnych prisťahovalcov, a to záchranou väčšieho počtu životov na mori;
- zvýšiť vnútornú bezpečnosť EÚ ako celku, a to prispením k prevencii cezhraničnej trestnej činnosti[286].

Systém začal fungovať 2. decembra 2013 vo všetkých členských štátoch s vonkajšími hranicami a od 1. decembra 2014 začne fungovať aj v ostatných členských štátoch. Nariadenie sa týka dozoru nad suchozemskými a morskými vonkajšími hranicami a vzdušnými hranicami členských štátov.

Colný informačný systém

Ďalším dôležitým spoločným informačným systémom zriadeným na úrovni EÚ je colný informačný systém (CIS)[287]. V rámci zriadenia vnútorného trhu boli zrušené

284 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.

285 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1168/2011 z 25. Októbra 2011, ktorým sa mení a dopĺňa nariadenie Rady (ES) č. 2007/2004 o zriadení Európskej agentúry pre riadenie operačnej spolupráce na vonkajších hraniciach členských štátov Európskej únie (*nariadenie o agentúre Frontex*), Ú. v. EÚ L 394, 2011.

286 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), KOM(2008) 68 v konečnom znení, Brusel, 13. februára 2008; Európska komisia (2011), Posúdenie vplyvu sprevádzajúce návrh 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.

287 Rada Európskej únie (1995), Akt Rady z 26. júla 1995 o využívaní informačných technológií na colné účely, Ú. v. EÚ C 316, 1995, zmenený dokumentom Rada Európskej únie (2009), Nariadenie Rady (ES) č. 515/1997 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.

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 systému CIS je pomáhať členským štátom pri prevencii, vyšetrovaní a stíhaní závažných porušení vnútroštátnych a európskych právnych predpisov v oblasti ciel a poľnohospodárstva.

Informácie uvedené v systéme CIS zahŕňajú osobné údaje s odkazom na zadržané, zachytené alebo skonfiškované komodity, dopravné prostriedky, podniky, osoby, tovar a hotovosť. 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 systému CIS je povolený vnútroštátnym colným a daňovým orgánom a orgánom v oblasti poľnohospodárstva a verejného zdravia, policajným orgánom, ako aj Europolu a Eurojustu.

Spracúvanie osobných údajov musí byť v súlade s osobitnými pravidlami stanovenými nariadením č. 515/1997 a dohovorom o systéme CIS[288], ako aj ustanoveniami smernice o ochrane údajov, nariadenia o ochrane údajov inštitúciami EÚ, dohovorom č. 108 a odporúčaním v oblasti policajných údajov. Európsky dozorný úradník je zodpovedný za dohľad nad súladom CIS s nariadením (ES) č. 45/2001 a zvoláva stretnutie najmenej raz do roka so všetkými vnútroštátnymi dozornými orgánmi kompetentnými v oblasti otázok dohľadu súvisiacich s CIS.

288 Tamtiež.

8

Ďalšie osobitné európske právne predpisy o ochrane údajov

EÚ	Zahrnuté otázky	Rada Európy
Smernica o ochrane údajov Smernica o súkromí v elektronických komunikáciách	Elektronické komunikácie	Dohovor č. 108 Odporúčanie o telekomunikačných službách
Smernica o ochrane údajov, článok 8 ods. 2 písm. b)	Zamestnanecké vzťahy	Dohovor č. 108 Odporúčanie o údajoch o zamestnaní
		ESĽP, *Copland/Spojenému kráľovstvu*, č. 62617/00, 3. apríla 2007
Smernica o ochrane údajov, článok 8 ods. 3	Zdravotné údaje	Dohovor č. 108 Odporúčanie o zdravotných údajoch
		ESĽP, *Z./Fínsko*, č. 22009/93, 25. februára 1997
Smernica o klinických skúšaniach	Klinické skúšania	
Smernica o ochrane údajov, článok 6 ods. 1 písm. b) a e), článok 13 ods. 2	Štatistiky	Dohovor č. 108 Odporúčanie o štatistických údajoch
Nariadenie (ES) č. 223/2009 o európskej štatistike SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland* , 16. decembra 2008	Oficiálne štatistiky	Dohovor č. 108 Odporúčanie o štatistických údajoch

Smernica 2004/39/ES o trhoch s finančnými nástrojmi Nariadenie (EÚ) č. 648/2012 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**	Dohovor č. 108 Odporúčanie 90(19) použité pre platby a ďalšie súvisiace operácie ESĽP, *Michaud/Francúzsko*, č. 12323/11, 6. decembra 2012

V niekoľkých prípadoch boli prijaté osobitné právne nástroje na európskej úrovni, ktorých prostredníctvom sa podrobnejšie uplatňujú všeobecné pravidlá dohovoru č. 108 alebo smernice o ochrane údajov v špecifických situáciách.

8.1. 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.
- Spracovanie osobných údajov v súvislosti s poskytovaním telekomunikačných služieb na úrovni EÚ je upravené smernicou o súkromí v elektronických komunikáciách.
- Dôvernosť elektronických komunikácií sa týka nielen obsahu komunikácie, ale aj prevádzkových 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 Rada Európy vydala odporúčanie na ochranu údajov v oblasti telekomunikácií, s osobitným zreteľom na telefonické služby[289]. Podľa tohto odporúčania

289 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.

by sa účely zberu a spracovania 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 vylúčili 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 v elektronických komunikáciách s cieľom doplniť a spresniť ustanovenia smernice o ochrane údajov pre telekomunikačný sektor[290]. Uplatňovanie smernice o súkromí v elektronických komunikáciách je obmedzené na komunikačné služby vo verejných elektronických sieťach.

V smernici o súkromí v 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;

- údaje nevyhnutne potrebné na nadviazanie a udržanie komunikácie, tzv. prevádzkové údaje, napríklad informácie o komunikujúcich partneroch, čase a dĺžke komunikácie;

- prevádzkové údaje zahŕňajú údaje, ktoré sa konkrétne týkajú umiestnenia komunikačného zariadenia, tzv. lokalizačné údaje; sú to zároveň údaje o mieste

290 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, smernicou 2002/58/ES týkajúcou sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadením (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, Ú. v. EÚ L 337, 2009.

používateľov komunikačných zariadení a majú osobitný význam pre používateľov mobilných komunikačných zariadení.

Poskytovateľ služieb môže používať prevádzkové údaje len pri fakturácii a technickom poskytovaní služby. Tieto údaje však môžu byť so súhlasom dotknutej osoby zverejnené 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.

Iný prístup k údajom o komunikáciách v elektronických sieťach, napríklad prístup na účely vyšetrovania trestných činov, musí podľa článku 15 smernice o súkromí v elektronických komunikáciách spĺňať požiadavky na oprávnené zasahovanie do práva na ochranu údajov, ako je stanovené v článku 8 ods. 2 EDĽP a potvrdené v článkoch 8 a 52 charty.

Zmenami smernice o súkromí v elektronických komunikáciách z roku 2009[291] sa zaviedli nasledujúce 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.

- Členským štátom bola uložená povinnosť poskytnúť opravné prostriedky proti porušeniu zákazu nevyžiadanej komunikácie[292].

- Nie je už možné používanie súborov cookies – softvéru, ktorý monitoruje a zaznamenáva činnosti používateľa počítača – bez súhlasu používateľa počítača.

291 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 2009 L 337.

292 Pozri zmenenú smernicu, článok 13.

> Spôsob poskytnutia a získania súhlasu by mal byť v záujme zaistenia dostatočnej ochrany podrobnejšie upravený vo vnútroštátnych právnych predpisoch[293].

Ak v dôsledku neoprávneného prístupu, straty alebo zničenia údajov dôjde k porušeniu ochrany údajov, ihneď o tom musí byť informovaný dozorný orgán. Ak je dôsledkom porušenia ochrany údajov možné poškodenie účastníkov, musia byť informovaní aj účastníci[294].

Smernicou o uchovávaní údajov, ktorá bola vyhlásená za neplatnú 8. apríla 2014,[295] bola poskytovateľom komunikačných služieb uložená povinnosť, aby uchovávali a sprístupnili prevádzkové údaje, a to konkrétne na účely boja proti závažnej trestnej činnosti, za obdobie minimálne šiestich, maximálne však 24 mesiacov, bez ohľadu na to, či poskytovateľ tieto údaje potreboval alebo nepotreboval na fakturačné účely alebo na technické poskytovanie služby.

Členské štáty EÚ zriadia nezávislé verejné orgány, ktoré zodpovedajú za monitorovanie bezpečnosti uchovávaných údajov.

Uchovávanie telekomunikačných údajov jasne zasahuje do práva na ochranu údajov[296]. Opodstatnenosť takéhoto zasahovania bola spochybnená v niekoľkých súdnych konaniach v členských štátoch EÚ.[297]

> Príklad: Vo veci *Digital Rights Ireland a Seitlinger a iní*[298] vyhlásil SDEÚ smernicu o o uchovávaní údajov za neplatnú. SDEÚ vyhlásil, že „rozsiahly a mimoriadne závažný zásah tejto smernice do predmetných základných práv nie je dosta-

293 Pozri tamtiež, článok 5; pozri tiež: pracovná skupina zriadená podľa článku 29 (2012), *stanovisko 04/2012 k vyňatiu z povinnosti získať súhlas s cookies,* WP 194, Brusel, 7. júna 2012.

294 Pozri tiež: pracovná skupina zriadená podľa článku 29 (2011), *pracovný dokument 01/2011 o platnom rámci EÚ týkajúcom sa porušenia bezpečnosti údajov a odporúčania pre budúci rozvoj politiky*, WP 184, Brusel, 5. apríla 2011.

295 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.

296 Európsky dozorný úradník pre ochranu údajov (2011), *stanovisko z 31. mája 2011 k hodnotiacej správe Komisie pre Radu a Európsky parlament o smernici o uchovávaní údajov (smernici 2006/24/ES)*, 31. mája 2011.

297 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.

298 Spojené veci C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a iní*, 8. apríla 2014, bod 65.

točne vymedzený, aby zabezpečoval, že sa uvedený zásah skutočne obmedzí na nevyhnutné minimum“.

Zásadnou otázkou v kontexte elektronických komunikácií je zasahovanie zo strany verejných orgánov. Prostriedky sledovania komunikáciami alebo ich odpočúvanie, napríklad odpočúvacími zariadeniami, sú prípustné len v prípade, že to umožňujú právne predpisy, a pokiaľ ide o nevyhnutné opatrenie v demokratickej spoločnosti v záujme: ochrany štátnej bezpečnosti, verejnej bezpečnosti a peňažných záujmov štátu alebo potláčania trestnej činnosti, alebo ochrany dotknutých osôb či práv a slobôd iných.

Príklad: Vo veci *Malone/Spojené kráľovstvo*[299] bol sťažovateľ obvinený z viacerých trestných činov týkajúcich sa nečestného zaobchádzania s odcudzeným tovarom. V priebehu súdneho procesu vyšlo najavo, že telefonické rozhovory sťažovateľa boli odpočúvané na základe príkazu vydaného ministrom vnútra. Napriek zákonnosti spôsobu odpočúvania komunikácie sťažovateľa z hľadiska vnútroštátnych právnych predpisov ESĽP konštatoval, že neexistovali žiadne zákonné predpisy týkajúce sa rozsahu a spôsobu vykonávania voľnej úvahy, ktorú môžu verejné orgány uplatňovať v tejto oblasti, a že zásah vyplývajúci z existencie danej praxe nebol „v súlade s právnymi predpismi“. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

8.2. Údaje o zamestnaní

Hlavné body

- Osobitné pravidlá pre ochranu údajov v zamestnaneckých vzťahoch sú uvedené v odporúčaní Rady Európy o údajoch o zamestnaní.
- V smernici o ochrane údajov sa zamestnanecké vzťahy osobitne uvádzajú len v súvislosti so spracúvaním citlivých údajov.
- 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.

299 ESĽP, *Malone/Spojené kráľovstvo*, č. 8691/79, 2. augusta 1984.

V EÚ neexistuje žiadny špecifický právny rámec, ktorým by sa upravovalo spracúvanie údajov v kontexte zamestnania. V smernici o ochrane údajov sa zamestnanecké vzťahy osobitne uvádzajú len v súvislosti s článkom 8 ods. 2 smernice, ktorý sa týka spracovania citlivých údajov. Pokiaľ ide o Radu Európy, odporúčanie o údajoch o zamestnaní bolo vydané v roku 1989 a v súčasnosti sa aktualizuje[300].

Prehľad najčastejších problémov v oblasti ochrany údajov týkajúcich sa zamestnania je uvedený v pracovnom dokumente pracovnej skupiny zriadenej podľa článku 29[301]. Pracovná skupina analyzovala význam súhlasu ako právneho základu pre spracovanie údajov o zamestnaní[302]. Zistila, že hospodárska nerovnováha medzi zamestnávateľom požadujúcim súhlas a zamestnancom, ktorý súhlas poskytuje, často vyvoláva pochybnosti o tom, či bol súhlas poskytnutý slobodne alebo nie. Pri posudzovaní platnosti súhlasu v súvislosti so zamestnaním teda treba dôkladne posúdiť okolnosti, za ktorých sa súhlas požaduje.

Bežný problém v oblasti ochrany údajov v súčasnom typickom pracovnom prostredí predstavuje legitímny rozsah monitorovania elektronickej komunikácie zamestnancov na pracovisku. Často sa tvrdí, že tento problém možno jednoducho vyriešiť zákazom súkromného používania služobných komunikačných prostriedkov. Takýto všeobecný zákaz by zrejme bol neprimeraný a nereálny. V tejto súvislosti je mimoriadne zaujímavý nasledujúci rozsudok ESĽP:

Príklad: Vo veci *Copland/Spojené kráľovstvo*[303] 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. ESĽP konštatoval, že telefonické hovory z budov podniku patria do rozsahu pojmov súkromný život a korešpondencia. Preto sú takéto hovory a e-maily zaslané zo zamestnania, ako aj informácie získané na základe monitorovania osobného používania internetu, chránené článkom 8 EDĽP. V prípade sťažovateľky neexistovali žiadne ustanovenia, ktorými by sa

300 Rada Európy, Výbor ministrov (1989), odporúčanie členským štátom Rec(89)2 o ochrane osobných údajov používaných na zamestnanecké účely, 18. januára 1989. Pozri tiež: poradný výbor pre dohovor č. 108, štúdia o odporúčaní č. R (89) 2 o ochrane osobných údajov používaných na zamestnanecké účely a na predloženie návrhu revízie uvedeného odporúčania, 9. septembra 2011.

301 Pracovná skupina zriadená podľa článku 29 (2001), *stanovisko 8/2001 k spracovaniu osobných údajov v súvislosti so zamestnaním*, WP 48, Brusel, 13. septembra 2001.

302 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.

303 ESĽP, *Copland/Spojené kráľovstvo*, č. 62617/00, 3. apríla 2007.

upravovali podmienky, za ktorých by zamestnávatelia mohli monitorovať používanie telefónu, e-mailu a internete zamestnancami. Zasahovanie teda nebolo v súlade s právnymi predpismi. Súd dospel k záveru, že došlo k porušeniu článku 8 EDĽP.

Podľa odporúčania Rady Európy o údajoch o zamestnaní by sa osobné údaje zbierané na účely zamestnania mali získavať priamo od jednotlivých zamestnancov.

Osobné údaje zbierané 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 nesmú nikoho urážať spôsobom, akým sú sformulované. Táto požiadavka vyplýva zo zásady prijateľného spracúvania a presnosti 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 pre zastupovanie zamestnaneckých záujmov.

Citlivé osobné údaje zozbierané na účely zamestnania sa smú spracúvať len v konkrétnych prípadoch a podľa bezpečnostných opatrení stanovených vo vnútroštátnych právnych predpisoch. Zamestnávatelia sa smú pýtať zamestnancov alebo uchádzačov o zamestnanie na ich zdravotný stav alebo ich lekársky vyšetriť len v prípade, že je to nevyhnutné na: určenie vhodnosti pre dané zamestnanie, splnenie požiadaviek preventívnej medicíny alebo umožnenie poskytnutia sociálnych príspevkov. Údaje týkajúce sa zdravia sa nesmú zbierať z iných zdrojov ako je príslušný zamestnanec, okrem prípadov získania výslovného a informovaného súhlasu alebo ak je to stanovené vnútroštátnymi právnymi predpismi.

Podľa odporúčania o údajoch o zamestnaní by zamestnanci mali byť informovaní o účele spracovania ich osobných údajov, type uložených osobných údajov, subjektoch, ktorým sa ich údaje pravidelne oznamujú, ako aj o účele a právnom základe takejto komunikácie. Zamestnávatelia by mali svojich zamestnancov vopred informovať o zavedení alebo prispôsobení automatizovaných systémov na spracúvanie osobných údajov zamestnancov alebo na monitorovanie ich pohybu či produktivity.

Zamestnanci musia mať právo na prístup k svojim údajom o zamestnaní, ako aj právo opravy alebo vymazania týchto údajov. Ak sa spracúvajú hodnotiace údaje, zamestnanci musia mať právo spochybniť 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 spochybnenie zamietnutia.

8.3. Zdravotné údaje

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 8 ods. 1 smernice o ochrane údajov a článku 6 dohovoru č. 108. Vzťahuje sa na ne teda prísnejší režim spracovania údajov ako na údaje, ktoré nie sú citlivé.

Príklad: Vo veci *Z./Fínsko*[304] 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 stigmu, ktorá v mnohých spoločnostiach súvisí s týmto ochorením. Súd preto dospel k záveru, že umožnenie prístupu 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 EDĽP.

304 ESĽP, *Z./Fínsko*, č. 22009/93, 25. februára 1997, odseky 94 a 112; pozri tiež ESĽR, *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 iní/Slovensko*, č. 32881/04, 28. apríla 2009; ESĽP, *Szuluk/Spojené kráľovstvo*, č. 36936/05, 2. júna 2009.

Článkom 8 ods. 3 smernice o ochrane údajov sa umožňuje spracúvanie zdravotných údajov, ak je to potrebné na preventívne medicínske účely, stanovenie diagnózy, poskytnutie starostlivosti alebo liečby alebo riadenie zdravotných služieb. Spracúvanie je povolené len vtedy, ak ho vykonáva profesionálny subjekt v odbore poskytovania zdravotnej starostlivosti, ktorý je viazaný povinnosťou služobného tajomstva, alebo osoba, na ktorú sa vzťahuje rovnocenná povinnosť[305].

V odporúčaní Rady Európy o zdravotných údajoch z roku 1997 sa podrobnejšie uplatňujú zásady dohovoru č. 108 na spracúvanie údajov v oblasti zdravotníctva[306]. Navrhnuté pravidlá sú v súlade s pravidlami smernice o ochrane údajov, pokiaľ ide o legitímne účely spracúvania zdravotných údajov, nevyhnutné záväzky služobného tajomstva osôb používajúcich zdravotné údaje a práva dotknutých osôb týkajúce sa transparentnosti, prístupu, opravy a výmazu. Okrem toho sa zdravotné údaje, ktoré zákonne spracúvajú profesionálni zdravotníci, nesmú prenášať orgánom presadzovania práva, okrem prípadov, keď sú poskytnuté „dostatočné záruky brániace zverejneniu, ktoré by nebolo zlučiteľné s rešpektovaním [...] súkromného života zaručeným článkom 8 EDĽP“[307].

Odporúčanie o zdravotných údajoch tiež obsahuje osobitné ustanovenia o zdravotných údajoch nenarodených detí a právne nespôsobilých osôb, ako aj o spracovaní genetických údajov. Výslovne sa uznáva, že vedecký výskum je dôvodom pre 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 anonymizované údaje, obsahuje článok 12 odporúčania o zdravotných údajoch.

Vhodným spôsobom uspokojenia vedeckých potrieb a súčasného zaistenia ochrany záujmov dotknutých pacientov môže byť pseudonymizácia. Koncepcia pseudonymizácie v kontexte ochrany údajov je podrobnejšie vysvetlená v oddiele 2.1.3.

Uskutočnila sa intenzívna diskusia na vnútroštátnej a európskej úrovni o iniciatívach na uchovávanie údajov o liečení pacientov v elektronických zdravotných súboroch[308]. Osobitným aspektom existencie celoštátnych systémov elektronických

305 Pozri tiež EDĽP, *Biriuk/Litva*, č. 23373/03, 25. novembra 2008.

306 Rada Európy, Výbor ministrov (1997), odporúčanie členským štátom Rec(97)5 o ochrane zdravotných údajov, 13. februára 1997.

307 ESĽP, č. 1585/09, *Avilkina a iní/Rusko*, 6. júna 2013, odseky 53 (nie je konečné).

308 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.

zdravotných súborov je ich cezhraničná dostupnosť: téma, ktorá je mimoriadne dôležitá v rámci EÚ v súvislosti s cezhraničnou zdravotnou starostlivosťou[309].

Ďalšou diskutovanou oblasťou týkajúcou sa nových ustanovení sú klinické skúšania, inými slovami skúšania nových liekov na pacientoch v rámci zdokumentovaného výskumného prostredia. Táto téma má významné dôsledky z hľadiska ochrany údajov. Klinické skúšania medicínskych produktov na použite u ľudí sú upravené smernicou Európskeho parlamentu a Rady 2001/20/ES zo 4. apríla 2001 o aproximácii zákonov, iných právnych predpisov a správnych opatrení členských štátov týkajúcich sa uplatňovania dobrej klinickej praxe počas klinických pokusov s humánnymi liekmi (*smernica o klinických skúšaniach*).[310] V decembri 2012 Európska komisia navrhla nariadenie, ktorým sa nahrádza smernica o klinických skúšaniach s cieľom väčšieho zjednotenia a zefektívnenia klinických skúšaní.[311]

Existuje veľa ďalších legislatívnych a iných iniciatív, ktoré sa riešia na úrovni EÚ, pokiaľ ide o osobné údaje v sektore zdravotníctva.[312]

8.4. Spracúvanie údajov na štatistické účely

Hlavné body

- Údaje zozbierané na štatistické účely sa nesmú použiť na žiadny iný účel.
- Údaje legitímne zozbierané na akýkoľvek účel sa môžu ďalej použiť na štatistické účely pod podmienkou, že vo vnútroštátnych právnych predpisoch sa stanovia primerané bezpečnostné opatrenia, ktoré budú používatelia dodržiavať. Na tento účel by sa predovšetkým malo počítať s anonymizáciou a pseudonymizáciou údajov pred prenosom tretím stranám.

309 Smernica Európskeho parlamentu a rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti, Ú. v. EÚ L 88, 2011.

310 Smernica Európskeho parlamentu a Rady 2001/20/ES zo 4. apríla 2001 o aproximácii zákonov, iných právnych predpisov a správnych opatrení členských štátov týkajúcich sa uplatňovania dobrej klinickej praxe počas klinických pokusov s humánnymi liekmi, Ú. v. L 121, 2001.

311 Európska komisia (2012), *návrh nariadenia Európskeho parlamentu a Rady o klinickom skúšaní liekov na humánne použitie, ktorým sa zrušuje smernica 2001/20/ES*, KOM(2012) 369 v konečnom znení, Brusel, 17. júla 2012.

312 Európsky dozorný úradník pre ochranu údajov (2013), *stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie Akčný plán elektronického zdravotníctva na roky 2012 – 2020: inovačná zdravotná starostlivosť pre 21. storočie*, Brusel, 27. marca 2013.

V smernici o ochrane údajov je spracúvanie údajov na štatistické účely uvedené v kontexte možných výnimiek zo zásad ochrany údajov. V článku 6 ods. 1 písm. b) smernice sa stanovuje, že vo vnútroštátnych právnych predpisoch je možné upustiť od zásady obmedzenia účelu v prospech ďalšieho použitia údajov na štatistické účely, ale vo vnútroštátnych právnych predpisoch sa zároveň musia stanoviť všetky nevyhnutné bezpečnostné opatrenia. Článkom 13 ods. 2 smernice sa umožňuje, aby sa vo vnútroštátnych právnych predpisoch obmedzili práva prístupu, ak sa údaje spracúvajú výlučne na štatistické účely, zároveň sa však v nich musia predpisovať primerané bezpečnostné opatrenia. V tejto súvislosti sa v smernici o ochrane údajov uvádza špecifická požiadavka, podľa ktorej sa žiadne údaje získané alebo vytvorené v rámci štatistického výskumu nesmú použiť pri prijímaní konkrétnych rozhodnutí o dotknutých osobách.

Prevádzkovateľ, ktorý zákonne zozbieral údaje na akýkoľvek účel, síce môže tieto údaje použiť na svoje vlastné štatistické účely (tzv. sekundárna štatistika), pred prenosom tretej strane na štatistické účely ich však bude musieť v závislosti od kontextu anonymizovať alebo pseudonymizovať, okrem prípadov, keď dotknutá osoba vyslovila súhlas s prenosom alebo je takýto prenos konkrétne ustanovený vo vnútroštátnych právnych predpisoch. Vyplýva to z požiadavky primeraných bezpečnostných opatrení podľa článku 6 ods.1 písm. b) smernice o ochrane údajov.

Najdôležitejšími prípadmi použitia údajov na štatistické účely sú oficiálne štatistiky realizované vnútroštátnymi a európskymi štatistickými úradmi na základe vnútroštátnych a európskych právnych predpisov o oficiálnej štatistike. Podľa týchto právnych predpisov sú občania a podniky zvyčajne povinní poskytnúť údaje štatistickým orgánom. Úradníci, ktorí pracujú v štatistických úradoch, sú viazaní osobitnými povinnosťami služobného tajomstva, ktoré sa prísne kontrolujú, keďže majú zásadný význam pre získanie vysokej úrovne dôvery občanov, ktorá je nevyhnutnou podmienkou sprístupnenia údajov štatistickým orgánom.

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 vnútroštátnej úrovni.[313] Nariadenie presadzuje zásadu, podľa ktorej oficiálne štatistické operácie potrebujú dostatočne presný právny základ.[314]

313 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.

314 Táto zásada sa spresňuje v kódexe postupov Eurostatu, ktorý v súlade s článkom 11 nariadenia o európskej štatistike poskytuje etické usmernenie, pokiaľ ide o spôsob vykonávania oficiálnej štatistiky vrátane ohľaduplného používania osobných údajov. Kódex je dostupný na adrese: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

Príklad: Vo veci *Huber/Nemecko*[315] SDEÚ konštatoval, že zber a uchovávanie osobných údajov vykonávané orgánom na štatistické účely nepredstavujú ako také dostatočný dôvod zákonnosti spracúvania. Právny predpis, v ktorom sa stanovuje spracúvanie osobných údajov, musí spĺňať aj požiadavku nevyhnutnosti, ktorá v tomto prípade nebola splnená.

V rámci Rady Európy bolo v roku 1997 vydané odporúčanie o štatistických údajoch, ktoré sa týka realizácie štatistiky vo verejnom a súkromnom sektore[316]. V uvedenom odporúčaní sa predkladajú zásady, ktoré sa zhodujú s hlavnými pravidlami smernice o ochrane údajov opísanými v predchádzajúcom texte. Odporúčanie obsahuje aj podrobnejšie pravidlá pre nasledujúce oblasti:

Údaje zozbierané prevádzkovateľom na štatistické účely sa nesmú použiť na žiadny iný účel, zatiaľ čo údaje zozbierané na iné ako štatistické účely možno sprístupniť na ďalšie štatistické použitie. V odporúčaní o štatistických údajoch sa dokonca umožňuje oznamovanie údajov tretím stranám, pokiaľ ide výlučne o štatistický účel. V takýchto prípadoch by sa strany mali dohodnúť a písomne stanoviť rozsah ďalšieho legitímneho použitia na štatistické účely. Keďže tento krok nemôže nahradiť súhlas dotknutej osoby, predpokladá sa, že vo vnútroštátnych právnych predpisoch existujú dodatočné primerané bezpečnostné opatrenia s cieľom minimalizovať riziká zneužitia osobných údajov, napríklad povinnosť anonymizovať alebo pseudonymizovať údaje pred prenosom.

Osoby, ktoré sa profesionálne venujú štatistickým výskumom, by mali byť na základe vnútroštátnych právnych predpisov viazané zvláštnymi povinnosťami služobného tajomstva (ako je to obvyklé pri oficiálnych štatistikách). Uvedené povinnosti by sa mali rozšíriť aj na pýtajúce sa osoby, ak sú zamestnané na účely zberu údajov od dotknutých alebo iných osôb.

Ak štatistický prieskum s použitím osobných údajov nevyplýva zo zákona a použitie údajov má byť legitímne, dotknuté osoby budú musieť vyjadriť súhlas s použitím svojich údajov, alebo im aspoň musí byť poskytnutá príležitosť vzniesť námietku. Ak sa osobné údaje zbierajú na štatistické účely formou rozhovorov s osobami, dopytované osoby musia byť jasne informované o tom, či zverejnenie údajov je alebo nie je povinné zo zákona. Citlivé údaje by sa nikdy nemali zbierať takým spôsobom, ktorý by umožňoval identifikáciu jednotlivca, pokiaľ sa to výslovne nepovoľuje vo vnútroštátnych právnych predpisoch.

315 SDEÚ, C-524/06, *Huber/Bundesrepublik Deutschland*, 16. decembra 2008, pozri predovšetkým bod 68.

316 Rada Európy, Výbor ministrov (1997), odporúčanie členským štátom Rec(97)18 o ochrane osobných údajov zbieraných a spracúvaných na štatistické účely, 30. septembra 1997.

Ak nie je možné uskutočniť štatistický prieskum s anonymnými údajmi a musia sa použiť osobné údaje, mali by sa údaje zozbierané na tento účel čo najskôr anonymizovať. Výsledky štatistického prieskumu minimálne nesmú umožňovať identifikáciu žiadnej dotknutej osoby, okrem prípadov, keď by identifikácia preukázateľne neznamenala 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 napríklad, že údaje by mali byť pseudonymizované a buď kódovací kľúč, alebo zoznam identifikačných synoným by sa mali uchovávať oddelene od pseudonymizovaných údajov.

8.5. Finančné údaje

Hlavné body

- Aj keď finančné údaje nie sú citlivými údajmi v zmysle dohovoru č. 108 alebo smernice o ochrane údajov, ich spracúvanie si vyžaduje osobitné bezpečnostné opatrenia na zaistenie presnosti a bezpečnosti údajov.
- Do elektronických platobných systémov musí byť zabudovaná ochrana údajov, tzv. ochrana súkromia v štádiu návrhu.
- Konkrétne problémy týkajúce sa ochrany údajov v tejto oblasti vznikajú v súvislosti s potrebou zaviesť vhodné mechanizmy autentifikácie.

Príklad: Vo veci *Michaud/Francúzsko*[317] sťažovateľ (francúzsky právnik) spochybnil povinnosť hlásiť podozrenia týkajúce sa možného prania špinavých peňazí zo strany klientov, ktorá je stanovená vo francúzskych právnych predpisoch. ESĽP konštatoval, že povinnosť právnikov, aby orgánom štátnej správy poskytovali informácie o inej osobe, ku ktorým získajú prístup na základe výmeny s danou osobou, predstavovala zasahovanie do práva právnikov na rešpektovanie ich korešpondencie a súkromného života podľa článku 8 EDĽP, keďže tento pojem zahŕňa činnosti profesijnej a obchodnej povahy. Dané zasahovanie však bolo

317 ESĽP, *Michaud/Francúzsko*, č. 12323/11, 6. decembra 2012; pozri tiež ESĽP, *Niemietz/Nemecko*, č. 13710/88, 16. decembra 1992, odsek 29 a ESĽP, *Halford/Spojené kráľovstvo*, *č. 20605/92,* 25. júna 1997, bod 42.

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 obmedzených okolností, ESĽP dospel k záveru, že táto povinnosť bola primeraná a že nedošlo k porušeniu článku 8.

Uplatňovaním všeobecného právneho rámca ochrany údajov zahrnutého do dohovoru č. 108 sa v kontexte platieb zaoberala Rada Európy v odporúčaní Rec(90)19 z roku 1990[318]. Vysvetľuje v ňom rozsah zákonného zberu a používania údajov v kontexte platieb, a to najmä prostredníctvom platobných kariet. Ďalej navrhuje zákonodarcom v jednotlivých členských štátoch podrobné predpisy týkajúce sa obmedzení pri oznamovaní platobných údajov tretím stranám, časových limitov uchovávania údajov, transparentnosti a bezpečnosti údajov a cezhraničných tokoch údajov, ako aj o dohľade a prostriedkoch nápravy. Navrhované riešenia zodpovedali riešeniam, ktoré boli neskôr predložené ako všeobecný rámec ochrany údajov v EÚ v rámci smernice o ochrane údajov.

Vzniká viacero právnych nástrojov týkajúcich sa regulácie trhov s finančnými nástrojmi a činnosti úverových inštitúcií a investičných podnikov[319]. Ďalšie právne nástroje pomáhajú v boji proti zneužitiu vnútorných informácií a manipulácii s trhom[320]. Medzi najzávažnejšie problémy v tejto oblasti, ktoré ovplyvňujú ochranu údajov, patria:

- uchovávanie záznamov o finančných transakciách;
- prenos osobných údajov do tretích krajín;

318 Rada Európy, Výbor ministrov (1990), odporúčanie č. R(90)19 o ochrane osobných údajov používaných pri platbách a ďalších súvisiacich operáciách, 13. septembra 1990.

319 Európska komisia (2011), *návrh smernice Európskeho parlamentu a Rady 2004/39/ES o trhoch s finančnými nástrojmi ktorou sa zrušuje smernica Európskeho parlamentu a Rady 2004/39*, KOM(2011) 656 v konečnom znení, Brusel, 20. októbra 2011; Európska komisia (2011), *návrh nariadenia Európskeho parlamentu a Rady o trhoch s finančnými nástrojmi, ktorým sa mení a dopĺňa nariadenie [EMIR] o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov*, KOM(2011) 652 v konečnom znení, Brusel, 20. októbra 2011; Európska komisia (2011), *návrh smernice Európskeho parlamentu a Rady o prístupe k činnosti úverových inštitúcií a o prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, ktorou sa mení a dopĺňa smernica Európskeho parlamentu a Rady 2002/87/ES zo 16. decembra 2002 o doplnkovom dohľade nad úverovými inštitúciami, poisťovňami a investičnými spoločnosťami vo finančnom konglomeráte*, KOM(2011) 453 v konečnom znení, Brusel, 20. júla 2011.

320 Európska komisia (2011), *návrh nariadenia Európskeho parlamentu a Rady o obchodovaní s využitím dôverných informácií a o manipulácii s trhom (zneužívanie trhu)*, KOM(2011) 651 v konečnom znení, Brusel, 20. októbra 2011; Európska komisia (2011), *návrh smernice Európskeho parlamentu a Rady o trestných sankciách za obchodovanie s využitím dôverných informácií a manipuláciu s trhom*, KOM(2011) 654 v konečnom znení, Brusel, 20. október 2011.

- nahrávanie telefonických rozhovorov alebo elektronickej komunikácie vrátane právomoci príslušných orgánov požadovať prevádzkové telefonické a dátové záznamy;

- zverejnenie osobných informácií vrátane uverejnenia postihov;

- dozorné a vyšetrovacie právomoci príslušných orgánov vrátane kontrol na mieste a vstupu do súkromných priestorov na zabavenie dokumentov;

- mechanizmy oznamovania porušení, t. j. systémy informátorov (tzv. whistle-blowing);

- spolupráca medzi príslušnými orgánmi členských štátov a Európskym orgánom pre cenné papiere a trhy (ESMA).

Existujú ďalšie problémy v týchto oblastiach, ktoré sa riešia osobitným spôsobom vrátane zberu údajov o finančnom postavení dotknutých osôb[321] alebo cezhraničných platbách prostredníctvom bankových prevodov, ktoré nutne vedú ku vzniku tokov osobných údajov[322].

321 Nariadenie Európskeho parlamentu a Rady (ES) č. 1060/2009 zo 16. septembra 2009 o ratingových agentúrach, Ú. v. EÚ L 302, 2009; Európska komisia, *návrh nariadenia Európskeho parlamentu a Rady o zmene a doplnení nariadenia (ES) č. 1060/2009 o ratingových agentúrach,* KOM(2010) 289 v konečnom znení, Brusel, 2. Júna 2010.

322 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.

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.

EDRi, *An introduction to data protection*, Brusel, dostupné na: www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Mníchovch, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Mníchov, C. H. Beck.

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. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antverpy, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and 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. and Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* Vol. 4, č. 5, d. 193 – 220, dostupné na: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press

Kapitola 2

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.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paríž, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and 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*, Vol. 57, č. 6, s. 1701–1777.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Mníchov, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, dostupné na: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Kapitoly 3 až 5

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. and Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Mníchov, 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.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

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.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, dostupné na www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Kapitola 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and 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

Kapitola 7

Europol (2012), *Data Protection at Europol*, Luxemburg, Úrad pre publikácie, dostupné na: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, Vol. 13, č. 3, s. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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*, Vol. 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, dostupné na: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Kapitola 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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*, Vol. 36, č. 5, s. 722–776.

Rosemary, J. and Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

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 iní/Slovensko, č. 32881/04, 28. apríla 2009
Leander/Švédsko, č. 9248/81, 26. marca 1987
Odièvre/Francúzsko [VK], č. 42326/98, 13. februára 2003

Vyvažovanie ochrany údajov so slobodou prejavu

Axel Springer AG/Nemecko, [VK], č. 39954/08, 7. Februára 2012
Von Hannover/Nemecko, č. 59320/00, 24. júna 2004
Von Hannover/Nemecko (č. 2) [VK], č. 40660/08 a 60641/08, 7. februára 2012

Problémy pri ochrane údajov on-line

K.U./Fínsko, č. 2872/02, 2. decembra 2008

Korešpondencia

Amann/Švajčiarsko [VK], č. 27798/95, 16. februára 2000
Bernh Larsen Holding AS a iní/Nórsko, č. 24117/08, 14. marca 2013
Cemalettin Canli/Turecko, č. 22427/04, 18. Novembra 2008

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
McMichael/Spojené kráľovstvo, č. 16424/90, 24. februára 1995
M.G./Spojené kráľovstvo, č. 39393/98, 24. septembra 2002
Rotaru/Rumunsko [VK], č. 28341/95, 4. Mája 2000
S. a Marper/ Spojené kráľovstvo, č. 30562/04 a 30566/04, 4. decembra 2008
Šimovolos/Rusko, č. 30194/09, 21. júna 2011
Turek/Slovensko, č. 57986/00, 14. februára 2006

Databázy registra trestov

B.B./Francúzsko, č. 5335/06, 17. decembra 2009
M.M./Spojené kráľovstvo, č. 24029/07, 13. novembra 2012

Databázy DNA

S. a Marper/Spojenému kráľovstvu, č. 30562/04 a 30566/04, 4. decembra 2008

Údaje GPS

Uzun/Nemecko, č. 35623/05, 2. septembra 2010

Údaje týkajúce sa zdravia

Biriuk/Litve, č. 23373/03, 25. novembra 2008
I./Fínsko, č. 20511/03, 17. júla 2008
L.L./Francúzsko, č. 7508/02, 10. októbra 2006
M.S./Švédsko, č. 34209/96, 2. júla 2002
Szuluk/Spojené kráľovstvo, č. 36936/05, 2. júna 2009
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

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
Copland/Spojené kráľovstvo, č. 62617/00, 3. apríla 2007
Cotlet/Rumunsko, č. 38565/97, 3. júna 2003
Kruslin/Francúzsko, č. 11801/85, 24. apríla 1990
Lambert/Francúzsko, č. 23618/94, 24. augusta 1998
Liberty a iní/Spojené kráľovstvo, č. 58243/00, 1. júla 2008
Malone/Spojené kráľovstvo, č. 8691/79, 26. apríla 1985
Halford/Spojené kráľovstvo, č. 20605/92, 25. júna 1997
Szuluk/Spojené kráľovstvo, č. 36936/05, 2. júna 2009

Povinnosti subjektov zodpovedných za zabezpečenie vykonávania práv

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

Fotografie

Sciacca/Taliansko, č. 50774/99, 11. januára 2005
Von Hannover/Nemecko, č. 59320/00, 24. júna 2004

Právo byť zabudnutý

Segerstedt-Wiberg a iní/Švédsko, č. 62332/00, 6. júna 2006

Právo námietky

Leander/Švédsko, č. 9248/81, 26. Marca 1987
Mosley/Spojené kráľovstvo, č. 48009/08, 10. mája 2011
M.S./Švédsko, č. 34209/96, 2. Júla 2002
Rotaru/Rumunsko [VK], č. 28341/95, 4. mája 2000

Citlivé kategórie údajov

I./Fínsko, č. 20511/03, 17. júla 2008

Michaud/Francúzsko, č. 12323/11, 6. decembra 2012
S. a Marper/Spojené kráľovstvo, č. 30562/04 a 30566/04, 4. decembra 2008

Dohľad a presadzovanie (úloha rôznych subjektov vrátane orgánov pre ochranu údajov)

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 „21 Décembre 1989" a iní/Rumunsko, č. 33810/07 a 18817/08, 24. mája 2011
Bykov/Rusko [VK], č. 4378/02, 10. marca 2009
Kennedy/Spojené kráľovstvo, č. 26839/05, 18. mája 2010
Klass a iní/Nemecko, č. 5029/71, 6. septembra 1978
Rotaru/Rumunsko [VK], č. 28341/95, 4. mája 2000
Taylor-Sabori/Spojené kráľovstvo, č. 47114/99, 22. októbra 2002
Uzun/Nemecko, č. 35623/05, 2. septembra 2010
Vetter/Francúzsko, č.59842/00, 31. mája 2005

Video sledovanie

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

C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy a Satamedia Oy*, 16. decembra 2008
[Pojem „žurnalistické činnosti" v zmysle článku 9 smernice o ochrane údajov]

Spojené veci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert/Land Hessen*, 9. Novembra 2010
[Proporcionalita právnej povinnosti uverejňovať osobné údaje o príjemcoch pomoci z určitých poľnohospodárskych fondov EÚ]

C-101/01, *Bodil Lindqvist*, 6. novembra 2003
[Legitímnosť uverejnenia údajov o súkromnom živote iných súkromnou osobou na internete]

C-131/12, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, Návrh na začatie prejudiciálneho konania od *Audiencia Nacional* (Španielsko) predložený 9. marca 2012, 25. mája 2012, prebiehajúce konanie
[Povinnosť poskytovateľov vyhľadávačov nezobrazovať na žiadosť dotknutej osoby osobné údaje vo výsledkoch vyhľadávania]

C-270/11, *Európska komisia/Švédske kráľovstvo*, 30. mája 2013
[Pokuta za nevykonávanie smernice]

C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, 29. Januára 2008
[Povinnosť poskytovateľov internetového pripojenia zverejniť totožnosť používateľov programov na výmenu súborov KaZaA združeniu na ochranu práv duševného vlastníctva]

SDEÚ, C-288/12, *Európska Komisia/Maďarsko*, 8. apríla 2014
[Legitímnosť zrušenia funkcie vnútroštátneho úradníka pre ochranu údajov]

C-291/12, *Michael Schwarz/Stadt Bochum*, Stanovisko generálneho advokáta, 13. Júna 2013
[Porušenie primárneho práva EÚ nariadením (ES) 2252/2004, ktorým sa stanovuje, že odtlačky prstov sa musia uchovávať v pasoch]

C-360/10, *SABAM/Netlog NV*, 16. februára 2012
[Povinnosť poskytovateľov sociálnych sietí predchádzať nezákonnému používaniu hudobných a audiovizuálnych diel používateľmi sietí]

Spojené veci C-465/00, C-138/01 a C-139/01, *Rechnungshof/Österreichischer Rundfunk a iní a Neukomm a Lauermann/Österreichischer Rundfunk*, 20. mája 2003
[Proporcionalita právnej povinnosti uverejňovať osobné údaje o platoch zamestnancov určitých kategórií inštitúcií súvisiacich s verejným sektorom]

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 – „legitímne záujmy iných" – vo vnútroštátnych právnych predpisoch]

C-518/07, *Európska komisia/Spolková republika Nemecko*, 9. Marca 2010
[Nezávislosť vnútroštátneho dozorného orgánu]

C-524/06, *Huber/Bundesrepublik Deutschland*, 16. decembra 2008
[Legitímnosť uchovávania údajov o cudzincoch v štatistickom registri]

C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*, 5. Mája 2011
[Nevyhnutnosť obnoveného súhlasu]

C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*, 7. mája 2009
[Právo prístupu dotknutej osoby]

Spojené veci C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a iní*, 8. Apríla 2014
[Porušenie primárneho práva EÚ smernicou o uchovávaní údajov]

C-614/10, *Európska komisia/Rakúska republika*, 16. októbra 2012
[Nezávislosť vnútroštátneho dozorného orgánu]

Judikatúra súvisiaca s nariadením o ochrane údajov inštitúciami EÚ

C-28/08 P, *Európska komisia/The Bavarian Lager Co. Ltd*, 29. júna 2010
[Prístup k dokumentom]

C-41/00 P, *Interporc Im- und Export GmbH/Komisii Európskych spoločenstiev*, 6. marca 2003
[Prístup k dokumentom]

F-35/08, *Dimitrios Pachtitis/Európska komisia*, 15. júna 2010
[Použitie osobných údajov v kontexte zamestnania v inštitúciách EÚ]

F-46/09, *V/Európsky parlament*, 5. júla 2011
[Použitie osobných údajov v kontexte zamestnania v inštitúciách EÚ]

Zoznam judikatúry

Judikatúra Európskeho súdneho dvora

Judikatúra Európskeho súdu pre ľudské práva

Judikatúra vnútroštátnych súdov

Agentúra Európskej únie pre základné práva
Európsky súd pre ľudské práva – Rada Európy

Príručka o európskom práve v oblasti ochrany údajov

2014 — 197 s. — 14,8 × 21 cm

ISBN 978-92-871-9937-9 (Rada Európy)
ISBN 978-92-9239-340-3 (FRA)
doi:10.2811/55893

Viac doplňujúcich informácií o Agentúre Európskej únie pre základné práva je k dispozícii na internete. Sú dostupné na webovej stránke agentúry FRA: fra.europa.eu.

Viac informácií o Rade Európy je dostupných na internetovej stránke: hub.coe.int.

Ďalšie informácie týkajúce sa judikatúry Európskeho súdu pre ľudské práva sú k dispozícii na internetových stránkach ESĽP: echr.coe.int. Vyhľadávač HUDOC umožňuje prístup k rozsudkom a rozhodnutiam v angličtine a/alebo vo francúzštine, prekladom do vybraných jazykov, mesačníku stručných informácií o prejednávaných prípadoch, tlačovým správam a ďalším informáciám o práci Súdu.

10.2811/55893
TK-01-13-772-SK-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Prudký rozvoj informačných a komunikačných technológií poukazuje na rastúcu potrebu rozsiahlej ochrany osobných údajov. Ochrana osobných údajov predstavuje právo zaručené nástrojmi Európskej únie (EÚ), ako aj Rady Európy. Technologický pokrok posúva napríklad hranice sledovania, odpočúvania komunikácie a uchovávania údajov, čo predstavuje vážnu výzvu z hľadiska práva na ochranu údajov. Cieľom tejto príručky je zoznámiť právnikov z praxe, ktorí sa nešpecializujú na otázky ochrany údajov, s touto oblasťou práva. Príručka obsahuje prehľad platného právneho rámca EÚ a Rady Európy. Vysvetľujú sa v nej kľúčové časti judikatúry a zhŕňa hlavné rozsudky Európskeho súdu pre ľudské práva (ESĽP) a Súdneho dvora Európskej únie (SDEÚ). Ak takáto judikatúra neexistuje, uvádzajú sa praktické príklady s hypotetickými scenármi. Stručne povedané, cieľom tejto príručky je pomôcť pri energickom a oduševnenom presadzovaní práva na ochranu údajov.

AGENTÚRA EURÓPSKEJ ÚNIE PRE ZÁKLADNÉ PRÁVA
Schwarzenbergplatz 11 – 1040 Viedeň – Rakúsko
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

RADA EURÓPY
EURÓPSKY SÚD PRE ĽUDSKÉ PRÁVA
67075 Štrasburg Cedex – Francúzsko
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Úrad pre publikácie
ISBN 978-92-871-9937-9 (Rada Európy)
ISBN 978-92-9239-340-3 (FRA)