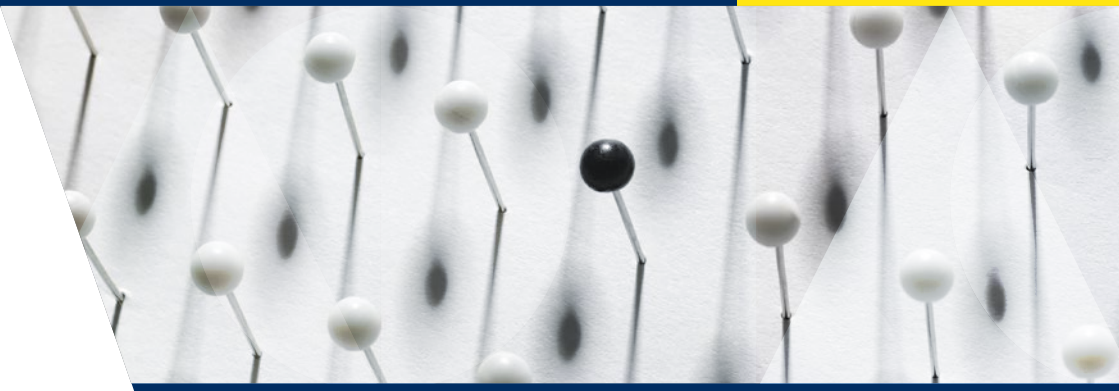
PŘÍRUČKA



Příručka evropského práva v oblasti ochrany osobních údajů

Vydání z roku 2018

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

EDPS

Rukopis této příručky byl dopsán v dubnu 2018.

V budoucnu budou k dispozici aktualizace na webových stránkách agentury FRA na adrese fra.europa.eu, na webových stránkách Rady Evropy na adrese coe.int/dataprotection, na webových stránkách Evropského soudu pro lidská práva v nabídce Case Law (Judikatura) na adrese echr.coe.int a na webových stránkách evropského inspektora ochrany údajů na adrese edps.europa.eu.

Fotografie (obálka a uvnitř publikace): © iStockphoto

Lucemburk: Úřad pro publikace Evropské unie, 2021

RE:	ISBN 978-92-871-9816-7		
FRA – Print:	ISBN 978-92-9474-445-6	doi:10.2811/904321	TK-05-17-225-CS-C
FRA – PDF:	ISBN 978-92-9474-444-9	doi:10.2811/28452	TK-05-17-225-CS-N

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

EDPS

Příručka evropského práva v oblasti ochrany osobních údajů

Vydání z roku 2018

Předmluva

Naše společnosti se stále více digitalizují. Tempo technologického vývoje a způsobu zpracovávání osobních údajů s ohledem na tyto změny denně ovlivňuje každého z nás, a to řadou různých způsobů. Právní rámce Evropské unie (EU) a Rady Evropy, které zaručují ochranu soukromí a osobních údajů, prošly v nedávné době přezkumem.

Evropa je průkopníkem ochrany údajů v celosvětovém měřítku. Normy EU na ochranu údajů vycházejí z Úmluvy Rady Evropy č. 108, z nástrojů EU – včetně obecného nařízení o ochraně osobních údajů a směrnice o ochraně údajů policií a trestním soudnictvím – jakož i z příslušné judikatury Evropského soudu pro lidská práva a Soudního dvora Evropské unie.

Reformy ochrany údajů, které provedla EU a Rada Evropy, jsou rozsáhlé a někdy složité, přinášejí však dalekosáhlé přínosy a mají vliv na jednotlivce a podniky. Cílem této příručky je zvýšit povědomí a zlepšit úroveň znalostí o pravidlech ochrany údajů, zejména v řadách právníků nespecialistů, kteří při své práci musejí řešit otázky spojené s ochranou osobních údajů.

Příručku vypracovala Agentura Evropské unie pro základní práva (FRA) spolu s Radou Evropy (ve spolupráci s Registrem Evropského soudu pro lidská práva) a evropským inspektorem ochrany údajů. Aktualizuje vydání z roku 2014 a je součástí řady právních příruček, na jejichž přípravě se podílela FRA a Rada Evropy.

Rádi bychom poděkovali orgánům pro ochranu údajů v Belgii, Estonsku, Francii, Gruzii, Irsku, Itálii, Maďarsku, Monaku, Švýcarsku a ve Spojeném království za jejich užitečnou zpětnou vazbu k pracovní verzi příručky. Dále bychom rádi vyjádřili uznání oddělení ochrany údajů při Evropské komisi a jeho oddělení pro mezinárodní toky dat a jejich ochranu. Děkujeme Soudnímu dvoru Evropské unie za podporu formou dokumentů poskytnutých během vypracovávání této příručky.

Závěrem bychom rádi vyjádřili dík Úřadu pro ochranu osobních údajů České republiky za podporu při revizi české verze této příručky.

Christos Giakoumopoulos

generální ředitel pro lidská práva a právní stát, Rada Evropy

Giovanni Buttarelli

evropský inspektor ochrany údajů

Michael O'Flaherty

ředitel Agentury Evropské unie pro základní práva

Obsah

Zkratky a akronymy

BCR	závazná podniková pravidla
CCTV	uzavřený televizní okruh
CETS	Řada smluv Rady Evropy
Listina	Listina základních práv Evropské unie
CIS	celní informační systém
SDEU	Soudní dvůr Evropské unie (před prosincem 2009 Evropský soudní dvůr, ESD)
RE	Rada Evropy
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy). Pozměňující protokol (CETS č. 223) k Úmluvě č. 108 („Modernizovaná úmluva č. 108“) přijal Výbor ministrů Rady Evropy u příležitosti svého 128. zasedání, které se konalo v dánském Elsinoru (17.–18. května 2018). Odkazy na „Modernizovanou úmluvu č. 108“ se týkají této úmluvy ve znění Protokolu CETS č. 223.
CRM	řízení vztahů se zákazníky
C-SIS	centrální schengenský informační systém
DPO	pověřenec pro ochranu osobních údajů
DPA	úřad pro ochranu osobních údajů
EZR	evropský zatýkací rozkaz
EDPB	Evropský sbor pro ochranu osobních údajů
ES	Evropské společenství
EÚLP	Evropská úmluva o lidských právech
ESLP	Evropský soud pro lidská práva
EIOÚ	evropský inspektor ochrany údajů
EHP	Evropský hospodářský prostor
EFSA	Evropský úřad pro bezpečnost potravin
ESVO	Evropské sdružení volného obchodu
ENISA	Agentura Evropské unie pro bezpečnost sítí a informací
ENU	národní jednotka Europolu

EPPO	Úřad evropského veřejného žalobce
ESMA	Evropský orgán pro cenné papíry a trhy
eTEN	transevropská telekomunikační síť
EU	Evropská unie
EuroPriSe	evropské osvědčení o zachování důvěrného charakteru informací
eu-LISA	Agentura EU pro rozsáhlé informační systémy
FRA	Agentura Evropské unie pro základní práva
GDPR	obecné nařízení o ochraně osobních údajů
GPS	globální polohový systém
ICCPR	Mezinárodní pakt o občanských a politických právech
IKT	informační a komunikační technologie
ISP	poskytovatel internetových služeb
JSB	společný kontrolní orgán
NGO	nevládní organizace
N-SIS	vnitrostátní schengenský informační systém
OECD	Organizace pro hospodářskou spolupráci a rozvoj
Úř. věst.	Úřední věstník
PIN	osobní identifikační číslo
PNR	jmenná evidence cestujících
SCG	Skupina pro koordinaci dohledu
SEPA	jednotná oblast pro platby v eurech
SIS	Schengenský informační systém
SWIFT	Společnost pro celosvětovou mezibankovní finanční telekomunikaci
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie
UDHR	Všeobecná deklarace lidských práv
OSN	Organizace spojených národů
VIS	Vízový informační systém

Jak používat tuto příručku

V této příručce se nastiňují právní normy týkající se ochrany osobních údajů, které stanovila Evropská unie (EU) a Rada Evropy (RE). Je koncipována tak, aby pomohla odborným pracovníkům, kteří se nespecializují na oblast ochrany údajů, včetně advokátů, soudců a jiných právnických povolání, jakož i osobám, které pracují pro jiné subjekty, například nevládní organizace (NGO), které mohou být nuceny se vypořádat s právními otázkami souvisejícími s ochranou údajů.

Slouží jako první referenční pomůcka v souvislosti s otázkami týkajícími se práva EU a Evropské úmluvy o lidských právech (EÚLP), jakož i Úmluvy RE o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108) a jiných nástrojů RE.

Každá kapitola je uvedena tabulkou, kde se určují právní ustanovení, která jsou relevantní k tématům, o nichž daná kapitola pojednává. Tabulky shrnují jak právo RE, tak právo EU a obsahují vybranou judikaturu Evropského soudu pro lidská práva (ESLP) a Soudního dvora Evropské unie (SDEU). Příslušné právní předpisy těchto dvou odlišných evropských struktur, které se týkají daných pojednávaných témat, jsou pak uvedeny jedny po druhých. Díky tomu může čtenář nahlédnout, kde se tyto dva právní systémy shodují a kde se rozcházejí. To by mělo také pomoci čtenářům najít klíčové informace pro jejich situaci, zejména pokud se řídí pouze judikaturou RE. V některých kapitolách, pokud to usnadňuje přehlednou prezentaci obsahu, se může pořadí témat v tabulkách mírně lišit od pořadí, v jakém jsou uvedena v kapitole samotné. Tato příručka rovněž nabízí stručný přehled rámce Organizace spojených národů.

Odborníci ze států, které nejsou členy EU, ale které jsou členskými státy RE a smluvní stranou EÚLP a Úmluvy č. 108, mohou získat přístup k informacím týkajícím se jejich vlastní země tak, že přeskočí rovnou na oddíly týkající se RE. Odborníci ze států, které nejsou členy EU, musí mít také na paměti, že od přijetí obecného nařízení EU o ochraně osobních údajů platí pravidla EU pro ochranu osobních údajů pro organizace a jiné subjekty, které nejsou usazeny v EU, pokud zpracovávají osobní údaje a nabízejí výrobky a služby subjektům údajů v Unii nebo sledují chování těchto subjektů údajů.

Odborníci z členských států EU budou muset nahlédnout do obou oddílů, protože tyto státy jsou vázány oběma právními řády. Je třeba podotknout, že reformy a modernizace pravidel ochrany údajů v Evropě, ať už byly podniknuty v rámci Rady

Evropy (Modernizovaná úmluva č. 108 ve znění Protokolu CETS č. 223), nebo EU (přijetí obecného nařízení o ochraně osobních údajů a směrnice (EU) 2016/680), byly provedeny souběžně. Regulační subjekty v obou právních systémech vynaložily maximální úsilí k tomu, aby zajistily soudržnost a slučitelnost obou právních rámců. Reformy tudíž přinesly větší harmonizaci mezi právem RE a EU v oblasti ochrany údajů. Osoby, které potřebují více informací o některém konkrétním problému, mohou najít seznam odbornějších materiálů v oddíle „Další literatura". Informace o ustanoveních Úmluvy č. 108 a jejího Dodatkového protokolu z roku 2001, která stále platí až do doby, kdy vstoupí v platnost pozměňující protokol, získá čtenář ve vydání této příručky z roku 2014.

Právo RE je představeno pomocí stručných odkazů na vybrané věci ESLP. Tyto věci byly vybrány z velkého počtu rozsudků a rozhodnutí ESLP týkajících se otázek v oblasti ochrany údajů.

K příslušným právním předpisům EU patří legislativní opatření, která byla přijata, relevantní ustanovení Smluv a Listina základních práv Evropské unie ve smyslu výkladu uvedeného v judikatuře SDEU. Kromě toho tato příručka nabízí stanoviska a pokyny přijaté pracovní skupinou zřízenou podle článku 29, což je poradní orgán pověřený směrnicí o ochraně údajů, aby poskytoval odborné poradenství členským státům EU. Počínaje 25. květnem 2018 bude nahrazena Evropským sborem pro ochranu osobních údajů (EDPB). Stanoviska evropského inspektora ochrany údajů rovněž nabízí důležitý vhled do výkladu práva EU, a jsou tudíž součástí této příručky.

Věci, které jsou popsány a citovány v této příručce, nabízí příklady významného souboru judikátů ESLP i SDEU. Cílem pokynů uvedených v závěru této příručky je pomoci čtenářům vyhledávat judikaturu on-line. Představená judikatura SDEU se týká starší směrnice o osobních údajích. Výklady SDEU jsou však i nadále platné pro příslušná práva a povinnosti stanovené v obecném nařízení o ochraně osobních údajů.

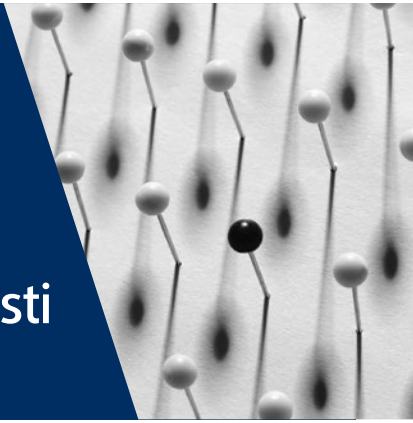
Kromě toho příručka nabízí i praktické příklady obsahující hypotetické scénáře, které čtenář najde v textových polích s modrým podkladem. Tyto příklady dále ilustrují uplatňování evropských pravidel ochrany údajů v praxi, zejména pokud neexistuje žádná v tomto konkrétním případě relevantní judikatura ESLP a SDEU. Jiné rámečky – na šedém podkladu – uvádějí příklady převzaté z jiných zdrojů, než je judikatura ESLP a SDEU, například právní předpisy a stanoviska vydaná pracovní skupinou zřízenou podle článku 29.

V úvodu této příručky je stručně popsána úloha obou právních systémů, které stanoví EÚLP a právo EU (kapitola 1). Kapitoly 2 až 10 pojednávají o těchto otázkách:

- terminologie v oblasti ochrany osobních údajů,
- hlavní zásady evropského práva v oblasti ochrany údajů,
- pravidla evropského práva v oblasti ochrany údajů,
- nezávislý dozor,
- práva subjektů údajů a jejich vynucování,
- přeshraniční předávání a toky osobních údajů,
- ochrana údajů v souvislosti s činností policie a trestního soudnictví,
- jiná evropská pravidla týkající se ochrany údajů ve specifických oblastech,
- moderní výzvy v oblasti ochrany osobních údajů.

1

Kontext a souvislosti evropského práva v oblasti ochrany údajů



EU	Pojednávaná témata	RE
Právo na ochranu údajů		
Smlouva o fungování Evropské unie, článek 16 Listina základních práv Evropské unie (dále jen „Listina"), článek 8 (právo na ochranu osobních údajů) Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice o ochraně údajů), Úř. věst. 1995 L 281 (v účinnosti do května 2018) Rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech, Úř. věst. 2008 L 350 (v účinnosti do května 2018) Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), Úř. věst. 2016 L 119		EÚLP, článek 8 (právo na respektování rodinného a soukromého života, obydlí a korespondence)

EU	Pojednávaná témata	RE
Směrnice (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (ochrana údajů pro policejní a justiční orgány), Úř. věst. 2016 L 119 Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. 2002 L 201 Nařízení (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (nařízení o ochraně údajů orgány EU), Úř. věst. 2001 L 8		Modernizovaná úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (Modernizovaná úmluva č. 108)
Omezení práva na ochranu osobních údajů		
Listina, čl. 52 odst. 1 Obecné nařízení o ochraně osobních údajů, článek 23 Rozsudek SDEU (velkého senátu) z roku 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*		EÚLP, čl. 8 odst. 2 Modernizovaná úmluva č. 108, článek 11 Rozsudek ESLP (velkého senátu) z roku 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04
Vyvážení práv		
Rozsudek SDEU (velkého senátu) z roku 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*	**Obecně**	
Rozsudek SDEU (velkého senátu) z roku 2008, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy a Satamedia Oy* Rozsudek SDEU (velkého senátu) z roku 2014, C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*	**Svoboda projevu**	Rozsudek ESLP (velkého senátu) z roku 2012, *Axel Springer AG v. Německo*, č. 39954/08 Rozsudek ESLP z roku 2011, *Mosley v. Spojené království*, č. 48009/08 Rozsudek ESLP z roku 2015, *Bohlen v. Německo*, č. 53495/09

EU	Pojednávaná témata	RE
Rozsudek SDEU (velkého senátu) z roku 2010, C-28/08 P, *Evropská komise v. The Bavarian Lager Co. Ltd* Rozsudek SDEU z roku 2015, C-615/13 P, *ClientEarth, PAN Europe v. EFSA*	Právo na přístup k dokumentům	Rozsudek ESLP (velkého senátu) z roku 2016, *Magyar Helsinki Bizottság v. Maďarsko*, č. 18030/11
Obecné nařízení o ochraně osobních údajů, článek 90	Služební tajemství	Rozsudek ESLP z roku 2015, *Pruteanu v. Rumunsko*, č. 30181/05
Obecné nařízení o ochraně osobních údajů, článek 91	Svoboda náboženského vyznání nebo přesvědčení	
	Svoboda umění a věd	Rozsudek ESLP z roku 2007, *Vereinigung bildender Künstler v. Rakousko*, č. 68345/01
Rozsudek SDEU (velkého senátu) z roku 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*	Ochrana majetku	
Rozsudek SDEU (velkého senátu) z roku 2014, C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* Rozsudek SDEU z roku 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*	Hospodářská práva	

1.1. Právo na ochranu osobních údajů

Hlavní body

- Podle článku 8 EÚLP tvoří právo jednotlivce na ochranu v souvislosti se zpracováním osobních údajů součást práva na respektování rodinného a soukromého života, obydlí a korespondence.
- Úmluva RE č. 108 je prvním a dosud jediným mezinárodním právně závazným nástrojem zabývajícím se ochranou údajů. Úmluva prošla procesem modernizace, který byl završen přijetím pozměňujícího protokolu CETS č. 223.
- V právu EU byla ochrana údajů uznána jako samostatné základní právo. To je stvrzeno v článku 16 Smlouvy o fungování EU i v článku 8 Listiny základních práv EU.

- V rámci práva EU byla ochrana údajů upravena vůbec poprvé směrnicí o ochraně údajů v roce 1995.
- Vzhledem k rychlému technologickému vývoji přijala EU v roce 2016 nový právní předpis, který měl upravit pravidla pro ochranu údajů s ohledem na potřeby digitální éry. Obecné nařízení o ochraně osobních údajů vstoupilo v platnost v květnu 2018 a zrušilo směrnici o ochraně údajů.
- Spolu s obecným nařízením o ochraně osobních údajů přijala EU právní předpis týkající se zpracování osobních údajů státními orgány pro účely prosazování práva. Směrnice (EU) 2016/680 stanoví pravidla ochrany údajů a zásady, kterými se řídí zpracování osobních údajů pro účely prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů.

1.1.1. Právo na respektování soukromého života a právo na ochranu osobních údajů: stručný úvod

Právo na respektování soukromého života a právo na ochranu osobních údajů spolu sice úzce souvisí, přesto se jedná o samostatná práva. Právo na soukromí – o kterém evropské právo hovoří jako o právu na respektování soukromého života – se do mezinárodního práva v oblasti lidských práv prosadilo ve Všeobecné deklaraci lidských práv, která byla přijata v roce 1948, jako jedno ze základních chráněných lidských práv. Krátce po přijetí Všeobecné deklarace lidských práv toto právo stvrdila i Evropa – v Evropské úmluvě o lidských právech (EÚLP), což je smlouva, která je pro smluvní strany právně závazná a která byla vypracována v roce 1950. EÚLP stanoví, že každý má právo na respektování svého rodinného a soukromého života, obydlí a korespondence. Zasahování do tohoto práva ze strany orgánu veřejné moci je zakázáno kromě případů, kdy je to v souladu se zákonem, sleduje důležité a legitimní veřejné zájmy a je to nezbytné v demokratické společnosti.

Všeobecná deklarace lidských práv a EÚLP byly přijaty dávno před rozvojem počítačů a internetu a nástupem informační společnosti. Tento vývoj přinesl jednotlivcům a společnosti značné výhody, zlepšil kvalitu života, efektivitu a produktivitu. Současně však představuje nová rizika pro právo na respektování soukromého života. V reakci na potřebu zvláštních pravidel, jimiž se řídí shromažďování a využívání osobních informací, vznikla nová koncepce soukromí, které se v některých

jurisdikcích říká „informační soukromí“ a v jiných „právo na informační sebeurčení“.[1] Tato koncepce měla za následek vypracování zvláštních právních předpisů, které stanoví ochranu osobních údajů.

S ochranou údajů se v Evropě začalo v 70. letech 20. století díky přijetí právních předpisů – v některých členských státech – umožňujících kontrolu zpracovávání osobních informací orgány veřejné moci a velkými podniky.[2] Nástroje na ochranu údajů pak byly přijaty i na evropské úrovni[3] a postupně se z ochrany údajů stala samostatná hodnota, která není součástí práva na respektování soukromého života. V právním řádu EU se ochrana údajů uznává jako základní právo, které je odlišné od základního práva na ochranu soukromého života. Toto rozdělení vyvolává otázky ohledně vztahu a rozdílů mezi oběma uvedenými právy.

Právo na respektování soukromého života a právo na ochranu osobních údajů spolu úzce souvisí. Obě usilují o ochranu podobných hodnot, tj. autonomie a lidské důstojnosti jednotlivce, a to tím, že mu zaručují osobní sféru, ve které může svobodně rozvíjet svou osobnost, přemýšlet a formovat své názory. Jsou tudíž základním předpokladem pro výkon ostatních základních svobod, jako je svoboda projevu, svoboda pokojného shromažďování a svoboda sdružovat se s jinými a svoboda náboženského vyznání.

Obě práva se liší svou formulací a oblastí působnosti. Právo na respektování soukromého života sestává z obecného zákazu zasahování, které podléhá určitým kritériím ve veřejném zájmu, která mohou v některých případech zásah odůvodnit. Ochrana

1 Německý spolkový ústavní soud potvrdil právo na informační sebeurčení v rozsudku z roku 1983, viz *Volkszählungsurteil*, BVerfGE Bd. 65, s. 1 a násl. Soud se domníval, že informační sebeurčení vyplývá ze základního práva na respektování osobnosti, které je chráněno německou ústavou. ESLP uznal v rozsudku z roku 2017, že článek 8 EÚLP „stanoví právo na jistou formu informačního sebeurčení“. Viz rozsudek ESLP (velkého senátu) ze dne 27. června 2017, *Satakunnan Markkinapörssi Oy a Satamedia Oy v. Finsko*, č. 931/13, bod 137.

2 První zákon o ochraně údajů přijala v roce 1970 německá spolková země Hesensko, platil však pouze v této spolkové zemi. První celostátní zákon na ochranu údajů na světě přijalo v roce 1973 Švédsko. Do konce 80. let 20. století přijalo právní předpis o ochraně osobních údajů několik evropských států (Francie, Německo, Nizozemsko a Spojené království).

3 Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108) byla přijata v roce 1981. EU přijala svůj první komplexní nástroj na ochranu údajů v roce 1995: směrnici 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

soukromých údajů se nahlíží jako moderní a aktivní právo[4], které zavádí systém brzd a protiváh na ochranu jednotlivců při zpracovávání jejich osobních údajů. Zpracování musí být v souladu se základními složkami ochrany osobních údajů, konkrétně pak s nezávislým dohledem a respektováním práv subjektu údajů.[5]

Článek 8 Listiny základních práv EU (dále jen „Listina") nejenže stvrzuje právo na ochranu osobních údajů, ale také vyjmenovává základní hodnoty, které jsou s tímto právem spojené. Stanoví, že zpracování osobních údajů musí být korektní, k přesně stanoveným účelům a založeno na souhlasu dotčené osoby nebo na jiném legitimním důvodu stanoveném zákonem. Jednotlivci musejí mít právo na přístup ke svým osobním údajům a právo na jejich opravu a na dodržování těchto pravidel musí dohlížet nezávislý orgán.

Právo na ochranu osobních údajů vstupuje do hry vždy, když probíhá zpracování osobních údajů; jedná se tudíž o širší právo než právo na respektování soukromého života. Veškeré operace zpracování osobních údajů musí zajišťovat vhodnou ochranu. Ochrana údajů se týká všech druhů osobních údajů a zpracování údajů, bez ohledu na souvislosti se soukromím a na dopad na ně. Zpracování osobních údajů může rovněž vést k porušování práva na soukromý život, jak je znázorněno v příkladu níže. Není však nutné prokázat narušení soukromého života, aby se začala uplatňovat pravidla pro zpracování údajů.

Právo na soukromí se týká situací, kdy byl narušen soukromý zájem nebo „soukromý život" jednotlivce. Jak je názorně ukázáno na různých místech v této příručce, koncepce „soukromého života" se široce vykládá v judikatuře tak, že zahrnuje intimní situace, citlivé nebo důvěrné informace, informace, které by mohly obrátit veřejné mínění proti jednotlivci, a dokonce aspekty profesního života jednotlivce a chování na veřejnosti. Avšak posouzení, zda došlo nebo nedošlo k zasahování do „soukromého života", závisí na kontextu a skutkovém stavu v každé věci.

Naproti tomu veškeré operace zahrnující zpracování osobních údajů by mohly spadat do působnosti pravidel ochrany údajů a vést k uplatnění práva na ochranu osobních údajů. Například pokud zaměstnavatel zaznamenává informace o jménech

4 Generální advokátka Sharpstonová popsala tuto situaci jako dvě samostatná práva: „tradiční" právo na ochranu soukromí a „modernější" právo, právo na ochranu údajů. Viz SDEU, *Stanovisko generální advokátky Sharpstonové* ze dne 17. června 2010, spojené věci C-92/09 a C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, bod 71.

5 Hustinx, P., Projevy a články EIOÚ, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* [Právo EU v oblasti ochrany údajů: přezkum směrnice 95/46/ES a navrhovaného obecného nařízení o ochraně osobních údajů], červenec 2013.

a odměnách vyplácených zaměstnancům, pouhé zaznamenávání těchto informací nelze považovat za zásah do soukromého života. Je však možné argumentovat, že se o takovýto zásah jedná v případě, že zaměstnavatel předal osobní informace zaměstnance třetí straně. Zaměstnanci musí v každém případě dodržovat pravidla ochrany údajů, protože zaznamenávání informací o zaměstnancích představuje zpracování údajů.

Příklad: Ve věci *Digital Rights Ireland*[6] byl SDEU požádán, aby rozhodl o platnosti směrnice 2006/24/ES s ohledem na základní práva na ochranu osobních údajů a respektování soukromého života, která jsou stvrzena v Listině základních práv EU. Směrnice ukládá poskytovatelům veřejně dostupných služeb elektronické komunikace nebo veřejným komunikačním sítím, aby uchovávali telekomunikační údaje občanů po dobu až dvou let, a to s cílem zajistit, aby údaje byly dostupné pro účely předcházení, vyšetřování a stíhání závažné trestné činnosti. Opatření se týkalo pouze metadat, lokačních údajů a údajů nezbytných k identifikaci předplatitele nebo uživatele. Netýkalo se obsahu elektronických komunikací.

SDEU považoval směrnici za zásah do základního práva na ochranu osobních údajů, „neboť upravuje zpracovávání osobních údajů".[7] Kromě toho dospěl k závěru, že směrnice zasahuje do práva na respektování soukromého života.[8] Jako celek osobní údaje uchovávané podle této směrnice, ke kterým by mohly mít přístup příslušné orgány, by mohly umožňovat vyvození „velmi přesn[ých] závěr[ů] o soukromém životě osob, jejichž údaje byly uchovány, tedy o každodenních zvyklostech, o místech, kde trvale či přechodně pobývají, o denních či jiných přesunech, o jejich aktivitách, společenských vztazích těchto osob a o společenských kruzích, s kterými se stýkají".[9] Zasahování do obou práv bylo rozsáhlé a mimořádně závažné.

6 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

7 Tamtéž, bod 36.

8 Tamtéž, body 32–35.

9 Tamtéž, bod 27.

SDEU prohlásil směrnici 2006/24/ES za neplatnou, ačkoliv sleduje legitimní cíl, protože konstatoval, že zásah do práv na ochranu osobních údajů a soukromého život byl závažný a nebyl omezen na kroky, které byly přísně vzato nezbytné.

1.1.2. Mezinárodní právní rámec: Organizace spojených národů

Rámec Organizace spojených národů neřadí ochranu osobních údajů mezi základní práva, ačkoliv právo na soukromí je již dlouhou dobu platným základním právem v mezinárodním právním řádu. Článek 12 Všeobecné deklarace lidských práv o respektování soukromého a rodinného života[10] byl vůbec prvním případem, kdy mezinárodní nástroj stanovil právo jednotlivce na ochranu své soukromé sféry před vniknutím jiných osob, zejména státu. Ačkoliv je Všeobecná deklarace lidských práv nezávazná, má nezanedbatelný status jako základní nástroj mezinárodního práva v oblasti lidských práv a ovlivnila vypracování jiných nástrojů v oblasti lidských práv v Evropě. Mezinárodní pakt o občanských a politických právech (ICCPR) vstoupil v platnost roku 1976. Stanoví se v něm, že nikdo nesmí být vystaven svévolnému nebo nezákonnému zasahování do soukromého života, do domova nebo korespondence ani nezákonným útokům na svou čest a pověst. ICCPR je mezinárodní smlouva, která zavazuje 169 stran, aby dodržovaly a zajišťovaly výkon občanských práv jednotlivců, včetně soukromí.

Od roku 2013 přijala Organizace spojených národů dvě rezoluce o otázkách soukromí s názvem „právo na soukromí v digitálním věku“[11] v reakci na vývoj nových technologií a na odhalení případů hromadného sledování, kterého se dopouštějí některé státy (Snowdenova odhalení). Důrazně se v nich odsuzuje hromadné sledování a zdůrazňuje se případný dopad takovéhoto sledování na základní právo na soukromí a na svobodu projevu a na fungování vitální a demokratické společnosti. Ačkoliv nejsou právně závazné, zažehly důležitou mezinárodní politickou diskusi na vysoké úrovni o soukromí, nových technologiích a sledování. Rovněž vedly ke zřízení pozice zvláštního zpravodaje pro právo na soukromí, který má mandát toto právo prosazovat a chránit. Ke zvláštním úkolům zpravodaje patří shromažďování

10 Organizace spojených národů (OSN), Všeobecná deklarace lidských práv, 10. prosince 1948.

11 Viz OSN, Valné shromáždění, Resolution on the right to privacy in the digital age [Rezoluce o právu na soukromí v digitálním věku], A/RES/68/167, New York, 18. prosince 2013; a OSN, Valné shromáždění, Revised draft resolution on the right to privacy in the digital age [Revidovaný návrh rezoluce o právu na soukromí v digitálním věku], A/C.3/69/L.26/Rev.1, New York, 19. listopadu 2014.

informací o vnitrostátních postupech a zkušenostech v souvislosti se soukromím a o výzvách, které přináší nové technologie, dále výměna a prosazování osvědčených postupů a určování případných překážek.

Zatímco dřívější rezoluce se zaměřovaly na negativní dopady hromadného sledování a odpovědnost států za omezení pravomocí zpravodajských orgánů, novější rezoluce jsou odrazem klíčového vývoje v diskusi o soukromí v rámci Organizace spojených národů.[12] Rezoluce přijaté v letech 2016 a 2017 stvrzují potřebu omezit pravomoci zpravodajských agentur a odsuzují hromadné sledování. Výslovně však také uvádějí, že „rostoucí schopnosti podniků shromažďovat, zpracovávat a využívat osobní údaje mohou představovat riziko pro výkon práva na soukromí v digitálním věku". Kromě odpovědnosti státních orgánů poukazují tudíž směrnice na odpovědnost soukromého sektoru za dodržování lidských práv a vyzývají podniky, aby informovaly uživatele o shromažďování, používání, sdílení a uchovávání osobních údajů a aby přijaly transparentní politiky ohledně zpracování.

1.1.3. Evropská úmluva o lidských právech

Rada Evropy vznikla v návaznosti na konec druhé světové války s cílem sdružovat státy Evropy a podporovat právní stát, demokracii, lidská práva a sociální rozvoj. Proto byla v roce 1950 přijata EÚLP, která vstoupila v platnost v roce 1953.

Smluvní strany mají mezinárodní povinnost se EÚLP řídit. Všichni členové RE již EÚLP začlenili do svého vnitrostátního práva nebo ji uplatňují, a proto musejí jednat v souladu s ustanoveními této úmluvy. Smluvní strany musejí dodržovat práva stanovená v úmluvě při výkonu veškeré činnosti nebo pravomocí. Sem patří též činnosti prováděné za účelem národní bezpečnosti. Přelomový rozsudek Evropského soudu pro lidská práva (ESLP) se týkal státní činnosti v citlivých oblastech práva a praxe národní bezpečnosti.[13] Soud bez váhání potvrdil, že činnosti v oblasti sledování představují zásah do respektování soukromého života.[14]

12 OSN, Valné shromáždění, Revised draft resolution on the right to privacy in the digital age [Revidovaný návrh rezoluce o právu na soukromí v digitálním věku], A/C.3/71/L.39/Rev.1, New York, 16. listopadu 2016; OSN, Rada pro lidská práva, The right to privacy in the digital age [Právo na soukromí v digitálním věku], A/HRC/34/L.7/Rev.1, 22. března 2017.

13 Viz například: Rozsudek ESLP ze dne 6. září 1978, *Klass a další v. Německo*, č. 5029/71; rozsudek ESLP (velkého senátu) ze dne 4. května 2000, *Rotaru v. Rumunsko*, č. 28341/95 a rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy v. Maďarsko*, č. 37138/14.

14 Tamtéž.

Aby se zajistilo, že smluvní strany dodržují své závazky vyplývající z EÚLP, byl v roce 1959 zřízen ve francouzském Štrasburku ESLP. ESLP zajišťuje, aby státy plnily své závazky stanovené úmluvou, protože projednává stížnosti jednotlivců, skupin jednotlivců, nevládních organizací nebo právnických osob, které tvrdí, že byla porušena úmluva. ESLP může rovněž zkoumat mezistátní věci předložené jedním nebo více členskými státy RE proti jinému členskému státu.

Od roku 2018 má Rada Evropy 47 smluvních států, z nichž 28 je též členskými státy EU. Stěžovatel u ESLP nemusí být státním příslušníkem jedné ze smluvních stran, ačkoliv k údajným porušením práva musí dojít v jurisdikci jedné ze smluvních stran.

Právo na ochranu osobních údajů tvoří součást práv chráněných podle článku 8 EÚLP, který zaručuje právo na respektování soukromého a rodinného života, obydlí a korespondence a stanoví podmínky, za nichž jsou povolena omezení tohoto práva.[15]

ESLP zkoumal řadu situací, které se týkaly otázek ochrany údajů. Patří k nim odposlech[16], různé formy sledování ze strany soukromého i veřejného sektoru[17] a ochrana před ukládáním osobních údajů orgány veřejné moci[18]. Právo na soukromý život není absolutní právo, protože výkon práva na soukromí by mohl ohrozit výkon jiných práv, např. svobody projevu a přístupu k informacím a opačně. Proto se soud snaží nalézt rovnováhu mezi dotčenými základními právy. Vyjasnil, že článek 8 EÚLP nejenže zavazuje státy k tomu, aby se zdržely jednání, které by mohlo porušovat toto právo stanovené úmluvou, ale že za určitých okolností mají pozitivní povinnost aktivně zaručit účinné respektování soukromého a rodinného života.[19] Podrobněji je řada těchto případů popsána v příslušných kapitolách.

1.1.4. Úmluva Rady Evropy č. 108

Po vzniku informační technologie v 60. letech 20. století bylo stále více zapotřebí stanovit podrobnější pravidla, která by ochránila jednotlivce prostřednictvím

15 Rada Evropy, Evropská úmluva o lidských právech, CETS č. 005, 1950.

16 Viz například: Rozsudek ESLP ze dne 2. srpna 1984, *Malone v. Spojené království*, č. 8691/79; rozsudek ESLP ze dne 3. dubna 2007, *Copland v. Spojené království*, č. 62617/00, nebo rozsudek ESLP ze dne 18. července 2017, *Mustafa Sezgin Tanrıkulu v. Turecko*, č. 27473/06.

17 Viz například: Rozsudek ESLP ze dne 6. září 1978, *Klass a další v. Německo*, č. 5029/71; rozsudek ESLP ze dne 2. září 2010, *Uzun v. Německo*, č. 35623/05.

18 Viz například: Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2015, *Roman Zakharov v. Rusko*, č. 47143/06; rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy v. Maďarsko*, č. 37138/14.

19 Viz například: Rozsudek ESLP ze dne 17. července 2008, *I v. Finsko*, č. 20511/03; rozsudek ESLP ze dne 2. prosince 2008, *K.U. v. Finsko*, č. 2872/02.

ochrany jejich osobních údajů. V polovině 70. let 20. století již byla Výborem ministrů Rady Evropy přijata různá usnesení týkající se ochrany osobních údajů, a to s odkazem na článek 8 EÚLP.[20] V roce 1981 byla nabídnuta k podpisu Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva č. 108)[21]. Úmluva č. 108 byla a stále je jediným právně závazným mezinárodním nástrojem v oblasti ochrany údajů.

Úmluva č. 108 se týká veškerého zpracování údajů, které provádí soukromý i veřejný sektor, včetně zpracování údajů ze strany soudních a donucovacích orgánů. Chrání osoby před porušením práva, s nímž může být zpracování osobních údajů spojeno, a současně usiluje o regulaci přeshraničních toků osobních údajů. Pokud jde o zpracování osobních údajů, zásady stanovené v této úmluvě se týkají zejména korektního a zákonného shromažďování a automatického zpracování údajů za konkrétními legitimními účely. To znamená, že údaje by neměly být používány k cílům, které nejsou s těmito účely slučitelné, a neměly by být uchovávány po dobu delší, než je nezbytné. Týkají se také kvality údajů, zejména toho, že údaje musejí být přiměřené, týkat se příslušných účelů a nesmí je překračovat (proporcionalita) a také musejí být přesné.

Úmluva kromě toho, že stanoví záruky zpracování osobních údajů a závazky v oblasti bezpečnosti údajů, zakazuje, nejsou-li zajištěny náležité právní záruky, zpracování „citlivých" údajů – například údajů o rase, politickém přesvědčení, zdravotním stavu, náboženském vyznání, sexuálním životě nebo trestněprávních záznamech dané osoby.

V úmluvě je rovněž zakotveno právo jednotlivce dozvědět se, že se o něm ukládají informace, a případně právo na jejich opravu. Omezení práv stanovených úmluvou je možné, pouze pokud je to dáno nadřazenými zájmy, např. bezpečností státu nebo jeho obranou. Kromě toho úmluva stanoví volný tok osobních informací mezi smluvními stranami a ukládá určitá omezení toků do států, kde právní úprava nestanoví rovnocennou ochranu.

20 Rada Evropy, Výbor ministrů (1973), Usnesení (73) 22 o ochraně soukromí jednotlivců v souvislosti s elektronickými databankami v soukromém sektoru, 26. září 1973; Rada Evropy, Výbor ministrů (1974), Usnesení (74) 29 o ochraně soukromí jednotlivců v souvislosti s elektronickými databankami ve veřejném sektoru, 20. září 1974.

21 Rada Evropy, Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, CETS č. 108, 1981.

Je třeba konstatovat, že Úmluva č. 108 je pro státy, které ji ratifikovaly, závazná. Nepodléhá soudnímu dohledu ESLP, ale byla vzata v potaz v judikatuře ESLP v souvislosti s článkem 8 EÚLP. V průběhu let soud rozhodl, že ochrana osobních údajů je důležitou součástí práva na respektování soukromého života (článek 8), a vycházel ze zásad Úmluvy č. 108 při určování, zda došlo nebo nedošlo do zásahu do tohoto základního práva.[22]

Výbor ministrů RE za účelem dalšího rozpracování obecných zásad a pravidel stanovených v Úmluvě č. 108 přijal několik právně nezávazných doporučení. Tato doporučení ovlivnila vývoj práva v oblasti ochrany údajů v Evropě. Kupříkladu doporučení o policii bylo dlouhá léta jediným nástrojem v Evropě, který stanovil pokyny k používání osobních údajů v policejním sektoru.[23] Zásady obsažené v tomto doporučení, například způsoby uchovávání souborů údajů a nutnost zavést jasná pravidla týkající se toho, kterým osobám je umožněn přístup k těmto souborům, byly dále rozpracovány a vychází z nich pozdější právní předpisy EU.[24] Pozdější doporučení se zaměřují na překonání výzev digitálního věku – například v souvislosti se zpracováním údajů v oblasti zaměstnanosti (viz kapitolu 9).

Všechny členské státy EU Úmluvu č. 108 ratifikovaly. V roce 1999 byly navrženy změny Úmluvy č. 108 s cílem umožnit EU, aby se stala smluvní stranou. Tyto změny však nikdy nevstoupily v platnost.[25] V roce 2001 byl přijat Dodatkový protokol k Úmluvě č. 108. Zavádí se jím ustanovení o přeshraničních tocích dat do zemí, které nejsou členskými státy, tzv. třetích zemí, a o povinném zřízení vnitrostátních orgánů dozoru nad zpracováním údajů.[26]

K Úmluvě č. 108 mohou přistoupit i státy, které nejsou smluvními stranami RE. Potenciál úmluvy jakožto všeobecné normy a její otevřenost jsou základem pro propagaci ochrany údajů na celosvětové úrovni. K dnešnímu dni je smluvní stranou

22 Viz například: Rozsudek ESLP ze dne 25. února 1997, *Z v. Finsko*, č. 22009/93.

23 Rada Evropy, Výbor ministrů (1987), Doporučení Rec(87)15 Výboru ministrů členským státům upravující používání osobních údajů v policejním sektoru, Štrasburk, 17. září 1987.

24 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. L 281, 23. listopadu 1995.

25 Rada Evropy, Změny Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č. 108) přijaté Výborem ministrů ve Štrasburku dne 15. června 1999.

26 Rada Evropy, Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, o orgánech dozoru a toku dat přes hranice, CETS č. 181, 2001. Po modernizaci Úmluvy č. 108 se tento protokol už neuplatňuje, protože byla aktualizována příslušná ustanovení a začleněna do Modernizované úmluvy č. 108.

Úmluvy č. 108 51 zemí. Patří k nim všechny členské státy Rady Evropy (47 zemí), Uruguay, první neevropská země, která přistoupila v srpnu 2013, a Mauricius, Senegal a Tunisko, které přistoupily v letech 2016 a 2017.

V nedávné době prošla úmluva procesem modernizace. Veřejná konzultace, která proběhla v roce 2011, potvrdila dva hlavní cíle této činnosti: zesílit ochranu soukromí v digitální oblasti a posílit kontrolní mechanismy úmluvy. Proces modernizace se zaměřil na tyto cíle a byl dokončen přijetím protokolu, kterým se mění Úmluva č. 108 (Protokol CETS č. 223). Činnost probíhala souběžně s dalšími reformami mezinárodních nástrojů v oblasti ochrany údajů a spolu s reformou pravidel EU v oblasti ochrany údajů, která byla zahájena v roce 2012. Regulační subjekty na úrovni Rady Evropy a EU vynaložily maximální úsilí k tomu, aby zajistily soudržnost a slučitelnost obou právních rámců. Modernizace zachovává všeobecnost a flexibilitu úmluvy a zvyšuje její potenciál coby všeobecného nástroje práva v oblasti ochrany údajů. Stvrzuje a upevňuje důležité zásady a stanoví nová práva pro jednotlivce a současně zpřísňuje povinnosti subjektů, které zpracovávají osobní údaje, a zajišťuje větší odpovědnost. Například osoby, jejich osobní údaje se zpracovávají, mají právo získat informace o důvodech tohoto zpracování údajů a mají právo vyjádřit proti tomuto zpracování námitku. V zájmu boje proti rostoucímu využívání profilování v internetovém světě úmluva také stanoví právo jednotlivce nepodléhat rozhodnutím, která jsou založena výlučně na automatizovaném zpracování, aniž by byla vzata v potaz stanoviska těchto osob. Účinné vynucování pravidel v oblasti ochrany osobních údajů ze strany nezávislých orgánů dozoru ve smluvních stranách se považuje za klíčový bod praktického provádění úmluvy. Proto modernizovaná úmluva zdůrazňuje, že je nutné, aby orgány dozoru měly účinné pravomoci a funkce a aby se těšily skutečné nezávislosti při plnění svého poslání.

1.1.5. Právo Evropské unie v oblasti ochrany údajů

Právo EU tvoří primární a sekundární právo EU. „Primární právo EU“ tvoří smlouvy, konkrétně pak Smlouva o Evropské unii (SEU) a Smlouva o fungování Evropské unie (SFEU), které byly ratifikovány všemi členskými státy EU. „Sekundární právo EU“ představují nařízení, směrnice a rozhodnutí EU, které byly přijaty orgány EU, jimž je tato pravomoc svěřena smlouvami.

Ochrana osobních údajů v primárním právu EU

Původní smlouvy Evropských společenství neobsahovaly žádnou zmínku o lidských právech a jejich ochraně, a to vzhledem k tomu, že Evropské hospodářské

společenství bylo původně koncipováno jako regionální organizace zaměřená na hospodářskou integraci a na vytvoření jednotného trhu. Základní zásada, na které byla založena a rozvíjena Evropská společenství – a která stejně tak platí dodnes –, je zásada svěření pravomocí. Podle této zásady jedná EU pouze v mezích pravomocí, které jí svěří členské státy, jak se uvádí ve smlouvách EU. Na rozdíl od Rady Evropy neobsahují smlouvy o EU žádnou výslovnou pravomoc v záležitostech týkajících se základních práv.

Jelikož však byly SDEU předkládány věci týkající se porušování lidských práv v oblastech, které jsou v působnosti práva EU, SDEU stanovil důležitý výklad smluv. Aby soud poskytl jednotlivcům ochranu, vnesl základní práva do takzvaných základních zásad evropského práva. Podle SDEU odrážejí tyto obecné zásady obsah ochrany lidských práv, který je uveden ve vnitrostátních ústavách a ve smlouvách o lidských právech, zejména EÚLP. SDEU konstatoval, že bude zajišťovat soulad práva EU s těmito zásadami.

EU uznala skutečnost, že by její politiky mohly mít dopad na lidská práva, a ve snaze propůjčit občanům pocit, že je jim EU „blíž", vyhlásila v roce 2000 Listinu základních práv Evropské unie (dále jen „Listina"). Je do ní začleněna celá řada občanských, politických, hospodářských a sociálních práv evropských občanů, a to syntézou ústavních tradic a mezinárodních závazků, které mají členské státy společné. Práva popsaná v Listině jsou rozdělena do šesti oddílů: důstojnost, svobody, rovnost, solidarita, občanská práva a soudnictví.

Ačkoliv se původně jednalo pouze o politický dokument, Listina se stala právně závaznou[27] jako součást primárního práva EU (viz čl. 6 odst. 1 SEU) se vstupem Lisabonské smlouvy v platnost dne 1. prosince 2009.[28] Ustanovení Listiny jsou určena orgánům a institucím EU a zavazují je dodržovat práva uvedená v Listině při plnění svých úkolů. Ustanovení Listiny jsou závazná i pro členské státy, a to když provádějí právo EU.

Listina nejenže zaručuje respektování soukromého a rodinného života (článek 7), ale také stanoví právo na ochranu osobních údajů (článek 8). Listina výslovně povyšuje úroveň této ochrany na úroveň základního práva v právu EU. Orgány a instituce EU musí toto právo zaručit a respektovat, stejně jako členské státy při uplatňování práva Unie (článek 51 Listiny). Článek 8 Listiny, který byl formulován několik let po přijetí

27 EU (2012), Listina základních práv Evropské unie, Úř. věst. 2012 C 326.

28 Viz Evropská společenství (2012), Smlouva o Evropské unii (konsolidované znění), Úř. věst. 2012 C 326; a Evropská společenství (2012), SFEU (konsolidované znění), Úř. věst. 2012 C 326.

směrnice o ochraně údajů, musí být chápán v tom smyslu, že je ztělesněním dřívějšího práva EU v oblasti ochrany údajů. Listina proto výslovně neuvádí právo na ochranu údajů v čl. 8 odst. 1, ale odkazuje na klíčové zásady v oblasti ochrany údajů v čl. 8 odst. 2. Ustanovení čl. 8 odst. 3 Listiny pak ukládá, že na uplatňování těchto zásad dohlíží nezávislý orgán.

Přijetí Lisabonské smlouvy je přelomové pro vývoj práva v oblasti ochrany údajů, nejen proto, že byla Listina povýšena mezi závazné právní dokumenty na úrovni primárního práva, ale také proto, že bylo přiznáno právo na ochranu osobních údajů. Toto právo je konkrétně uvedeno v článku 16 SFEU v části smlouvy věnované obecným zásadám EU. Článek 16 také vytváří nový právní základ a udílí EU pravomoc přijímat právní předpisy v oblasti ochrany údajů. Jedná se o významnou změnu, protože pravidla EU v oblasti ochrany údajů – zejména směrnice o ochraně údajů – byla původně založena na právním základu pro vnitřní trh a na nutnosti sblížit vnitrostátní právní řády tak, aby nebyla omezována svoboda pohybu údajů v EU. Článek 16 SFEU nyní nabízí nezávislý právní základ pro moderní, komplexní přístup k ochraně údajů, který zahrnuje všechny oblasti pravomocí EU, včetně policejní a soudní spolupráce v trestních věcech. Článek 16 SFEU rovněž stvrzuje, že dodržování pravidel ochrany údajů přijatých podle tohoto článku musí podléhat kontrole nezávislými orgány dozoru. Článek 16 posloužil jako právní základ pro přijetí komplexní reformy pravidel ochrany údajů v roce 2016, tj. obecného nařízení o ochraně osobních údajů a směrnice o ochraně údajů policií a trestním soudnictvím (viz níže).

Obecné nařízení o ochraně osobních údajů

Od roku 1995 do května 2018 byla hlavním právním nástrojem EU v oblasti ochrany údajů směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice o ochraně údajů).[29] Byla přijata v roce 1995, v době, kdy již několik členských států přijalo vnitrostátní zákony týkající se ochrany údajů,[30] a její přijetí bylo vyvoláno potřebou tyto zákony harmonizovat s cílem zajistit vysokou úroveň ochrany a volný pohyb osobních údajů mezi jednotlivými členskými státy. Volný pohyb zboží, kapitálu, služeb a osob na jednotném trhu vyžaduje volný

29 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. 1995 L 281.

30 První zákon o ochraně údajů na světě přijala v roce 1970 německá spolková země Hesensko, platil však pouze v této spolkové zemi. Švédsko přijalo zákon *Datalagen* v roce 1973, Německo přijalo zákon *Bundesdatenschutzgestez* v roce 1976 a Francie přijala zákon *Loi relatif à l'informatique, aux fichiers et aux libertés* v roce 1977. V roce 1984 byl ve Spojeném království přijat Data Protection Act [zákon o ochraně údajů]. Dále pak Nizozemsko přijalo v roce 1989 *Wet Persoonregistraties*.

pohyb údajů, kterého by nebylo možné dosáhnout, nebudou-li členské státy spoléhat na jednotnou, vysokou úroveň ochrany údajů.

Směrnice o ochraně údajů vychází ze zásad ochrany údajů, které již byly obsaženy ve vnitrostátních právních předpisech a v Úmluvě č. 108, ale často je rozpracovává. Využívá možnosti, kterou stanovil článek 11 Úmluvy č. 108, spočívající v doplnění nástrojů ochrany. Zejména zavedení nezávislého dozoru do směrnice je nástrojem ke zvýšení souladu s pravidly na ochranu údajů, který se ukázal jako významný příspěvek k účinnému fungování evropského práva v oblasti ochrany osobních údajů. Tento prvek byl tudíž začleněn do práva RE v roce 2001 formou Dodatkového protokolu k Úmluvě č. 108. Tato skutečnost dokládá v průběhu let úzkou interakci a pozitivní vliv obou nástrojů na sebe navzájem.

Směrnice o ochraně údajů stanoví podrobný a komplexní systém ochrany údajů v EU. V souladu s právním systémem EU se však směrnice neuplatňují přímo, ale musí být provedeny do vnitrostátních právních řádů členských států. Při provádění ustanovení směrnice mají členské státy nevyhnutelně prostor pro vlastní uvážení. I když měla směrnice zajistit úplnou harmonizaci[31] (a plnou míru ochrany), v praxi byla provedena ve členských státech odlišně. Vznikla tedy v celé EU rozmanitá pravidla ochrany údajů a definice a pravidla byly ve vnitrostátních právních předpisech vykládány různě. Rovněž se v jednotlivých členských státech lišila míra prosazování práva a přísnost sankcí. V neposlední řadě došlo od návrhu směrnice v polovině 90. let 20. století k významným změnám v oblasti informačních technologií. Jako celek vedly tyto důvody k reformě právních předpisů EU v oblasti ochrany údajů.

Reforma měla v dubnu 2016 po několika letech intenzivní diskuse za následek přijetí obecného nařízení o ochraně osobních údajů. Debaty o nutnosti modernizovat pravidla EU v oblasti ochrany údajů započaly v roce 2009, kdy Komise zahájila veřejnou konzultaci o budoucnosti právního rámce pro základní právo na ochranu osobních údajů. Návrh nařízení zveřejnila Komise v lednu 2012, čímž byl zahájen dlouhý legislativní proces jednání mezi Evropským parlamentem a Radou EU. Po přijetí stanovilo obecné nařízení o ochraně osobních údajů dvouleté přechodné období. Plně účinné začalo být dne 25. května 2018, kdy byla zrušena směrnice o ochraně údajů.

Přijetí obecného nařízení o ochraně osobních údajů v roce 2016 modernizovalo právní předpisy EU v oblasti ochrany údajů, zajistilo jejich přiměřenost, pokud jde

31 Rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, bod 29.

o ochranu základních práv v souvislosti s hospodářskými a sociálními výzvami digitálního věku. Nařízení GDPR zachovává a rozvíjí základní zásady a práva subjektu údajů stanovené ve směrnici o ochraně údajů. Kromě toho zavádí nové povinnosti, podle kterých organizace musejí zavést záměrnou a standardní ochranu údajů, za určitých okolností jmenovat pověřence pro ochranu osobních údajů, dodržovat nové právo na přenositelnost údajů a respektovat zásadu odpovědnosti. Podle práva EU jsou nařízení přímo použitelná, není tedy nutné je provádět do vnitrostátního práva. Obecné nařízení o ochraně osobních údajů tudíž stanoví jednotný soubor pravidel pro ochranu údajů v celé EU. Tím se vytvoří soudržná pravidla pro ochranu údajů v celé EU a vznikne prostředí právní jistoty, z čehož mohou těžit hospodářské subjekty a jednotlivci jakožto „subjekty údajů".

Ačkoliv je však obecné nařízení o ochraně osobních údajů přímo použitelné, očekává se, že členské státy upraví své současné vnitrostátní předpisy o ochraně údajů tak, aby byly plně v souladu s tímto nařízením, avšak zohlednily současně prostor pro vlastní uvážení u konkrétních ustanovení, jak je uvedeno v 10. bodě odůvodnění. Hlavní pravidla a zásady stanovené v tomto nařízení a silná práva, která nařízení přiznává jednotlivců, tvoří velkou část této příručky a jsou představeny v následujících kapitolách. Nařízení obsahuje komplexní pravidla týkající se územní působnosti. Platí pro podniky usazené v EU a také platí pro správce nebo zpracovatele, kteří nejsou usazeni v EU, ale nabízejí výrobky nebo služby subjektům údajů v EU nebo sledují jejich chování. Jelikož několik zahraničních technologických podniků má na evropském trhu klíčový podíl a miliony zákazníků v EU, je podrobení těchto organizací pravidlům EU v oblasti ochrany údajů důležité, aby byla zajištěna ochrana jednotlivců, jakož i rovné podmínky.

Ochrana údajů v oblasti prosazování práva – směrnice (EU) 2016/680

Zrušená směrnice o ochraně údajů stanovila komplexní režim ochrany údajů. Tento režim je nyní dále posílen přijetím obecného nařízení o ochraně osobních údajů. Ačkoliv byla zrušená směrnice o ochraně údajů komplexní, její oblast působnosti byla omezena na činnosti, které spadají pod vnitřní trh, a na činnosti orgánů veřejné moci s výjimkou donucovacích orgánů. Přijetí zvláštních nástrojů bylo tedy nutné k dosažení nezbytné jasnosti a rovnováhy mezi ochranou údajů a jinými legitimními zájmy a k překonání výzev, které jsou pro daná odvětví zvlášť relevantní. Tak je tomu i v případě pravidel upravujících zpracování osobních údajů donucovacími orgány.

První právní nástroj EU, který tuto záležitost upravoval, bylo rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech. Tato pravidla se vztahovala na výměnu policejních a soudních údajů mezi členskými státy. Vnitrostátní zpracování osobních údajů donucovacími orgány bylo z oblasti působnosti rozhodnutí vyňato.

Směrnice (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů,[32] označovaná též jako směrnice o ochraně údajů policií a trestním soudnictvím, tuto situaci napravila. Směrnice, přijatá souběžně s obecným nařízením o ochraně osobních údajů, zrušila rámcové rozhodnutí 2008/977/SVV a zavedla komplexní systém ochrany osobních údajů v kontextu prosazování práva a současně uznala zvláštnosti zpracování údajů v souvislosti s veřejnou bezpečností. Zatímco obecné nařízení o ochraně osobních údajů stanoví obecná pravidla na ochranu jednotlivců v souvislosti se zpracováním jejich osobních údajů a na zajištění volného pohybu těchto údajů v EU, směrnice stanoví zvláštní pravidla pro ochranu údajů v oblasti soudní spolupráce v trestněprávních věcech a v oblasti policejní spolupráce. Pokud příslušný orgán zpracovává osobní údaje pro účely prevence, vyšetřování, odhalování či stíhání trestných činů, použije se směrnice (EU) 2016/680. Pokud příslušné orgány zpracovávají osobní údaje pro jiné účely, než jsou ty výše uvedené, použije se obecný režim podle obecného nařízení o ochraně osobních údajů. Na rozdíl od svého předchůdce (rámcového rozhodnutí Rady 2008/977/SVV) se oblast působnosti směrnice (EU) 2016/680 rozšiřuje na vnitrostátní zpracování osobních údajů donucovacími orgány a není omezena na výměny těchto údajů mezi členskými státy. Kromě toho směrnice usiluje o nalezení rovnováhy mezi právy jednotlivců a legitimními zájmy zpracování v souvislosti s bezpečností.

Proto směrnice stvrzuje právo na ochranu osobních údajů a hlavní zásady, které by měly zahrnovat zpracování údajů, a to důsledně v souladu s pravidly a zásadami zakotvenými v obecném nařízení o ochraně osobních údajů. Práva jednotlivců a závazky uložené správcům – například v souvislosti se zabezpečením údajů, záměrnou a standardní ochranou údajů a ohlašováním případů porušení zabezpečení osobních údajů – připomínají práva a povinnosti uvedené v obecném nařízení o ochraně osobních údajů. Směrnice rovněž zohledňuje závažné nové technologické

32 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů, Úř. věst. L 119, 4. května 2016.

výzvy, které mohou mít zvlášť zatěžující dopad na jednotlivce, a pokouší se je řešit. Například jde o používání technik profilování ze strany donucovacích orgánů. V zásadě je nutné zakázat rozhodnutí založená výhradně na automatickém zpracování, včetně profilování.[33] Kromě toho nesmějí být založena na citlivých osobních údajích. Z těchto zásad platí určité výjimky uvedené ve směrnici. Dále toto zpracování nesmí mít za následek diskriminaci jakékoliv osoby.[34]

Směrnice také obsahuje pravidla zajišťující odpovědnost správců. Musejí jmenovat pověřence pro ochranu osobních údajů, který bude sledovat dodržování předpisů v oblasti ochrany údajů, informovat a poskytovat poradenství danému subjektu a zaměstnancům provádějícím zpracování ohledně jejich povinností a spolupracovat s dozorovým orgánem. Zpracování osobních údajů v policejním sektoru a v sektoru trestního soudnictví nyní podléhá dozoru ze strany nezávislých dozorových úřadů. Všeobecný i zvláštní režim právní ochrany údajů ve věcech prosazování práva a v trestněprávních věcech musí stejnou měrou dodržovat povinnosti uložené v Listině základních práv EU.

Zvláštní režim zpracování údajů v souvislosti s policejní a justiční spoluprací, který byl zřízen směrnicí o ochraně údajů policií a trestním soudnictvím, je podrobně popsán v kapitole 8.

Směrnice o soukromí a elektronických komunikacích

Rovněž se považovalo za nezbytné stanovit zvláštní pravidla v oblasti ochrany osobních údajů v odvětví elektronických komunikací. S rozvojem internetu a telefonování pomocí pevné linky a mobilních telefonů bylo důležité zajistit, že budou dodržována práva uživatelů na soukromí a důvěrnost. Směrnice 2002/58/ES[35] týkající se zpracování osobních údajů a ochrany soukromí v elektronických komunikacích (směrnice o soukromí a elektronických komunikacích) stanoví pravidla týkající se bezpečnosti osobních údajů v těchto sítích, oznamování porušení bezpečnosti osobních údajů a důvěrnosti komunikací.

Pokud jde o zabezpečení, musejí operátoři služeb elektronické komunikace zajistit kromě jiného, aby byl přístup k osobním údajům omezen pouze na oprávněné

33 Směrnice o ochraně údajů policií a trestním soudnictvím, čl. 11 odst. 1.

34 Tamtéž, čl. 11 odst. 2 a 3.

35 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, Úř. věst. L 201 (směrnice o soukromí a elektronických komunikacích).

osoby, a přijmout opatření s cílem zabránit zničení osobních údajů, jejich ztrátě nebo nezáměrnému poškození.[36] Existuje-li zvláštní riziko, že bude narušena bezpečnost veřejné komunikační sítě, musí operátoři informovat účastníky o tomto riziku.[37] Pokud navzdory provedeným bezpečnostním opatřením dojde k porušení bezpečnosti, musí operátoři uvědomit příslušný vnitrostátní orgán pověřený prováděním a vynucováním směrnice o tomto porušení bezpečnosti osobních údajů. Operátoři někdy také musejí oznámit případy porušení bezpečnosti osobních údajů jednotlivcům, zejména pokud takovéto porušení pravděpodobně negativně ovlivní jejich osobní údaje nebo soukromí.[38] Důvěrnost sdělení vyžaduje, aby byl zásadně zakázán příposlech, odposlech, uchovávání nebo jiné druhy zachycování sdělení a metadat. Směrnice také zakazuje nevyžádaná sdělení (často označovaná jako „spam"), ledaže k tomu uživatelé vyslovili souhlas, a obsahuje pravidla na ukládání „cookies" na počítačích a zařízeních. Tyto hlavní negativní povinnosti svědčí o tom, že důvěrnost sdělení je významnou měrou spojena s ochranou práva na respektování soukromého života, které je zakotveno v článku 7 Listiny, a práva na ochranu osobních údajů zakotveného v článku 8 Listiny.

V lednu 2017 Komise zveřejnila návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích, které by mělo nahradit směrnici o soukromí a elektronických komunikacích. Cílem reformy je sladit pravidla, jimiž se řídí elektronické komunikace, s novým režimem ochrany údajů, jejž stanovilo obecné nařízení o ochraně osobních údajů. Nové nařízení bude přímo použitelné v celé EU, všichni jednotlivci se budou těšit stejné úrovni ochrany svých elektronických komunikací, zatímco telekomunikační operátoři a podniky budou těžit z jasnosti, právní jistoty a existence jednotného souboru pravidel v celé EU. Navrhovaná pravidla týkající se důvěrnosti elektronických komunikací se rovněž použijí na nové subjekty poskytující služby elektronických komunikací, na které se nevztahuje směrnice o soukromí a elektronických komunikacích. Tato směrnice se týkala pouze poskytovatelů tradičních telekomunikačních služeb. Vzhledem k hromadnému rozšíření používání služeb, jako je Skype, WhatsApp, Facebook Messenger a Viber, k zasílání zpráv nebo k hovorům, budou tyto služby „over-the-top" (služby OTT) nyní spadat do působnosti tohoto nařízení a budou muset splňovat jeho požadavky na ochranu údajů, soukromí a zabezpečení. V době zveřejnění této příručky procházejí tato pravidla o elektronickém soukromí stále legislativním postupem.

36 Směrnice o soukromí a elektronických komunikacích, čl. 4 odst. 1.

37 Tamtéž, čl. 4 odst. 2.

38 Tamtéž, čl. 4 odst. 3.

Nařízení (ES) č. 45/2001

Jelikož směrnice o ochraně údajů mohla platit pouze pro členské státy EU, bylo třeba jiného právního nástroje s cílem stanovit ochranu údajů pro zpracování osobních údajů ze strany orgánů a institucí EU. Tento úkol plní nařízení (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (nařízení o ochraně údajů orgány EU).[39]

Nařízení (ES) č. 45/2001 se důsledně řídí zásadami všeobecného režimu ochrany údajů EU a uplatňuje tyto zásady na zpracování údajů prováděné orgány a institucemi EU při plnění svých úkolů. Kromě toho zřizuje nezávislý dozorový úřad za účelem sledování uplatňování ustanovení tohoto nařízení, tedy evropského inspektora ochrany údajů (EIOÚ). EIOÚ jsou svěřeny pravomoci v oblasti dozoru a povinnost sledovat zpracování osobních údajů v orgánech a institucích EU a vyslechnout a posoudit stížnosti na údajné porušení pravidel ochrany údajů. Rovněž poskytuje poradenství orgánům a institucím EU ve všech věcech týkajících se ochrany osobních údajů, a to počínaje návrhy nových právních předpisů až po vypracování interních pravidel zpracování údajů.

V lednu 2017 představila Evropská komise návrh nového nařízení o zpracování údajů orgány EU, kterým se ruší současné nařízení. Stejně jako v případě reformy směrnice o soukromí a elektronických komunikacích reforma nařízení (ES) č. 45/2001 zmodernizuje a uvede pravidla v souladu s novým režimem ochrany, jejž stanoví obecné nařízení o ochraně osobních údajů.

Úloha SDEU

SDEU má soudní příslušnost k rozhodování, zda některý členský stát plní nebo neplní své závazky podle práva EU v oblasti ochrany údajů, a k výkladu právních předpisů EU s cílem zajistit jejich účinné a jednotné uplatňování ve všech členských státech. Od přijetí směrnice o ochraně údajů v roce 1995 se nashromáždil významný objem judikatury, která objasňuje oblast působnosti a význam zásad ochrany údajů a základního práva na ochranu osobních údajů, které je zakotveno v článku 8 Listiny. Ačkoliv byla směrnice zrušena a nyní platí nový právní nástroj – obecné nařízení o ochraně osobních údajů –, stávající judikatura je stále relevantní a platná, pokud jde

39 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

o výklad a uplatňování zásad ochrany údajů EU, a to v rozsahu, v jakém byly v nařízení GDPR zachovány hlavní zásady a koncepce směrnice o ochraně údajů.

1.2. Omezení práva na ochranu osobních údajů

Hlavní body

- Právo na ochranu osobních údajů není absolutní právo. Může být omezeno, pokud je to nezbytné v obecném zájmu, nebo za účelem ochrany práv a svobod jiných osob.
- Podmínky pro omezení práva na respektování soukromého života a práva na ochranu osobních údajů jsou uvedeny v článku 8 EÚLP a v čl. 52 odst. 1 Listiny. Byly rozpracovány a vyloženy judikaturou ESLP a SDEU.
- Podle práva RE v oblasti ochrany údajů představuje zpracovávání osobních údajů zákonný zásah do práva na respektování soukromého života a lze je provést, pouze pokud:
  - je v souladu se zákonem,
  - sleduje legitimní cíl,
  - dodržuje podstatu základních práv a svobod,
  - je nezbytné a přiměřené v demokratické společnosti za účelem dosažení legitimního účelu.
- Právní řád EU ukládá podobné podmínky ohledně omezení výkonu základních práv, která jsou chráněna Listinou. Veškerá omezení všech základních práv, včetně ochrany osobních údajů, mohou být zákonná pouze tehdy, když:
  - jsou v souladu se zákonem,
  - dodržují podstatu tohoto práva,
  - jsou nezbytná s ohledem na zásadu proporcionality a
  - sledují cíl obecného zájmu uznaný EU nebo potřebu chránit práva jiných osob.

Základní právo na ochranu osobních údajů podle článku 8 Listiny není právem absolutním, „ale musí k němu být přihlédnuto ve vztahu k jeho funkci ve společnosti“.[40] Článek 52 odst. 1 Listiny tudíž připouští, že výkon práv může podléhat omezením, například těm, která jsou stanovena v článku 7 a 8 Listiny, za předpokladu, že tato omezení jsou stanovena zákonem, respektují podstatu uvedených práv a svobod a, při dodržení zásady proporcionality, jsou nezbytná a skutečně odpovídají cílům obecného zájmu, které uznává EU, nebo potřebě ochrany práv a svobod druhého.[41] Obdobně je v systému EÚLP zaručena ochrana údajů článkem 8 a výkon tohoto práva může být omezen, pokud je to nezbytné k plnění legitimního účelu. Tento oddíl se zaměřuje na podmínky zásahu podle EÚLP, jak je vyložila judikatura ESLP, ale také na podmínky zákonného omezení podle článku 52 Listiny.

1.2.1. Podmínky pro odůvodněnost zásahu podle EÚLP

Zpracování osobních údajů může představovat zásah do práva subjektu údajů na respektování soukromého života, které je chráněno článkem 8 EÚLP.[42] Jak je vysvětleno výše (viz oddíl 1.1.1 a oddíl 1.1.4), na rozdíl od právního řádu EU nestvrzuje EÚLP ochranu osobních údajů jako samostatné základní právo. Místo toho tvoří ochrana osobních údajů součást práv chráněných v rámci práva na respektování soukromého života. Ne každá operace zahrnující zpracování osobních údajů tedy spadá do působnosti článku 8 EÚLP. Aby se uplatnil článek 8, je nejprve třeba určit, zda byl narušen soukromý zájem nebo soukromý život určité osoby. Prostřednictvím judikatury ESLP rozpracoval pojem „soukromý život“ do podoby široké koncepce zahrnující dokonce i aspekty pracovního života a vystupování na veřejnosti. Rozhodl také, že ochrana osobních údajů je důležitou součástí práva na respektování soukromého života. Avšak navzdory širokému výkladu soukromého života nepředstavují samy o sobě všechny druhy zpracování narušení práv chráněných článkem 8.

Pokud se ESLP domnívá, že dotčená operace zpracování má dopad na právo jednotlivce na respektování soukromého života, přezkoumá, zda je zásah odůvodněný. Právo na respektování soukromého života není absolutním právem, ale musí být

40 Viz například rozsudek SDEU (velkého senátu) ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, bod 48.

41 Tamtéž, bod 50.

42 Rozsudek ESLP (velkého senátu) ze dne 8. prosince 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04, bod 67.

vyváženo a posuzováno s ohledem na jiné legitimní zájmy a práva, ať už jiných osob (soukromé zájmy) nebo společnosti jako celku (veřejné zájmy).

Toto jsou kumulativní podmínky, při jejichž splnění může být zásah odůvodněný:

V souladu se zákonem

Podle judikatury ESLP je zásah v souladu se zákonem, pokud je založen na ustanovení vnitrostátního práva, které vykazuje jisté vlastnosti. Zákon musí být „přístupný dotčeným osobám a jeho důsledky musí být předvídatelné".[43] Předvídatelné je takové pravidlo, které „je formulováno s dostatečnou přesností, která umožní každému jednotlivci – v nutných případech i po vyhledání vhodného poradenství – upravit své jednání".[44] Kromě toho „míra přesnosti vyžadovaná ‚zákonem' v této souvislosti závisí na konkrétní skutkové podstatě".[45]

Příklady: Ve věci *Rotaru v. Rumunsko*[46] stěžovatel uváděl porušení svého práva na respektování soukromého života z toho důvodu, že rumunská zpravodajská služba vlastnila a využívala spis obsahující jeho osobní informace. ESLP konstatoval, že i když vnitrostátní právo umožňuje shromažďovat, zaznamenávat a archivovat tajné spisy s informacemi, které mají dopad na národní bezpečnost, nestanoví žádná omezení týkající se výkonu těchto pravomocí, které jsou i nadále na vlastním uvážení daných orgánů. Vnitrostátní právo například neurčilo druh informací, které by mohly být zpracovány, kategorie osob, proti kterým je možné uplatnit opatření v oblasti sledování, okolnosti, za kterých je možné tato opatření přijmout, a postup, který je třeba

43 Rozsudek ESLP (velkého senátu) ze dne 16. února 2000, *Amann v. Švýcarsko*, č. 27798/95, bod 50; viz též rozsudek ESLP ze dne 25. března 1998, *Kopp v. Švýcarsko*, č. 23224/94, bod 55 a rozsudek ESLP ze dne 10. února 2009, *Iordachi a další v. Moldavsko*, č. 25198/02, bod 50.

44 Rozsudek ESLP (velkého senátu) ze dne 16. února 2000, *Amann v. Švýcarsko*, č. 27798/95, bod 56; viz též rozsudek ESLP ze dne 2. srpna 1984, *Malone v. Spojené království*, č. 8691/79, bod 66; rozsudek ESLP ze dne 25. března 1983, *Silver a další v. Spojené království*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, bod 88.

45 Rozsudek ESLP ze dne 26. dubna 1979, *The Sunday Times v. Spojené království*, č. 6538/74, bod 49; viz také rozsudek ESLP ze dne 25. března 1983, *Silver a další v. Spojené království*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, bod 88.

46 Rozsudek ESLP (velkého senátu) ze dne 4. května 2000, *Rotaru v. Rumunsko*, č. 28341/95, bod 57; viz též rozsudek ESLP ze dne 28. června 2007, *Association for European Integration and Human Rights a Ekimdzhiev v. Bulharsko*, č. 62540/00; rozsudek ESLP ze dne 21. června 2011, *Shimovolos v. Rusko*, č. 30194/09; a rozsudek ESLP ze dne 31. května 2005, *Vetter v. Francie*, č. 59842/00.

uplatnit. Soud proto dospěl k závěru, že vnitrostátní právo není v souladu s požadavkem předvídatelnosti podle článku 8 EÚLP a že došlo k porušení tohoto článku.

Ve věci *Taylor-Sabori v. Spojené království*[47] byl stěžovatel sledován policií. Za pomoci „klonu" stěžovatelova pageru byla policie schopna odposlouchávat zprávy, které mu byly zaslány. Stěžovatel byl zatčen a obviněn ze spolčování s cílem zajistit dodávku drogy podléhající regulaci. Součástí spisu státního zástupce proti němu byly soudobé písemné záznamy o zprávách na jeho pageru, které policie přepsala. V době konání soudního procesu se stěžovatelem však britské právo neobsahovalo žádné ustanovení týkající se odposlouchávání sdělení zaslaných pomocí soukromého telekomunikačního systému. Zásah do jeho práv tudíž nebyl „v souladu se zákonem". ESLP rozhodl, že došlo k porušení článku 8 EÚLP.

Věc *Vukota-Bojić v. Švýcarsko*[48] se týkala tajného sledování žadatele o sociální pojištění soukromými detektivy najatými stěžovatelovou pojišťovnou. ESLP měl za to, že i když dotčené opatření týkající se sledování stěžovatele objednala soukromá pojišťovna, této společnosti udělil stát právo vyplácet dávky na základě povinného zdravotního pojištění a právo vybírat pojistné. Stát se nemůže zprostit zodpovědnosti podle úmluvy tím, že své povinnosti přenese na soukromé subjekty nebo osoby. Vnitrostátní právo musí stanovit dostatečné záruky proti zneužívání, aby byl zásah do práv chráněných článkem 8 EÚLP „v souladu se zákonem". V dané věci ESLP rozhodl, že došlo k porušení článku 8 EÚLP, protože vnitrostátní právo neurčilo jasně rozsah a způsob výkonu vlastního uvážení přiznaného pojišťovnám vystupujícím jako veřejné orgány ve sporech o pojištění k provádění tajného sledování pojištěné osoby. Zejména pak nezahrnovalo dostatečné záruky proti zneužívání.

Sleduje legitimní cíl

Legitimní cíl může být buď jeden z vyjmenovaných veřejných zájmů, nebo ochrana práv a svobod jiných. Legitimní cíle, které by mohly zásah odůvodnit, jsou podle čl. 8 odst. 2 EÚLP zájmy národní bezpečnosti, veřejné bezpečnosti nebo hospodářský blahobyt země, ochrana pořádku, předcházení nepokojům nebo zločinnosti, ochrana zdraví nebo morálky a ochrana práv a svobod jiných.

47 Rozsudek ESLP ze dne 22. října 2002, *Taylor-Sabori v. Spojené království*, č. 47114/99.

48 Rozsudek ESLP ze dne 18. října 2016, *Vukota-Bojić v. Švýcarsko*, č. 61838/10, bod 77.

Příklad: Ve věci *Peck v. Spojené království*[49] se stěžovatel pokusil o sebevraždu na ulici tím, že si podřezal zápěstí, aniž by si byl vědom toho, že ho natáčí kamera CCTV. Policie, která sledovala kamery CCTV, ho zachránila a následně předala záznam CCTV sdělovacím prostředkům, které jej zveřejnily, aniž by zamaskovaly stěžovatelovu tvář. ESLP konstatoval, že neexistovaly žádné relevantní nebo dostatečné důvody, které by odůvodňovaly přímé zpřístupnění záznamu ze strany orgánů veřejnosti bez předchozího získání souhlasu stěžovatele nebo bez zamaskování jeho totožnosti. Soud proto shledal, že došlo k porušení článku 8 EÚLP.

Nezbytný v demokratické společnosti

ESLP uvedl, že „pojem nezbytnosti znamená, že zásah odpovídá naléhavé společenské potřebě, a zejména že je přiměřený legitimnímu cíli, který je sledován".[50] Při posuzování, zda je opatření nezbytné k uspokojení naléhavé společenské potřeby, přezkoumává ESLP jeho relevantnost a vhodnost s ohledem na sledovaný cíl. Za tímto účelem může zohlednit, zda se zásah pokouší vyřešit problém, který – pokud by nebyl řešen – by mohl mít škodlivý účinek na společnost, zda existují důkazy, že by zásah mohl zmírnit takovýto nepříznivý účinek, a jaká širší společenská hlediska jsou v dané věci ve hře.[51] Například shromažďování a ukládání osobních údajů konkrétních jednotlivců, o nichž bylo zjištěno, že mají vazby na teroristická hnutí, ze strany bezpečnostních složek by bylo zásahem do práva jednotlivců na respektování soukromého života, který by nicméně sloužil závažné a naléhavé společenské potřebě: národní bezpečnosti a boji proti terorismu. Má-li být splněna zkouška nezbytnosti, bude zásah také muset být přiměřený. V judikatuře ESLP se přiměřenost pojednává v rámci pojmu nezbytnosti. Podmínkou přiměřenosti je, aby zásah do práv chráněných EÚLP nepřekračoval hranice toho, co je nutné pro splnění sledovaného legitimního cíle. Významnými faktory, které je třeba zohlednit při provádění zkoušky přiměřenosti, je rozsah zásahu, zejména počet dotčených osob, a zavedené záruky nebo varování, které mají omezit rozsah nebo nepříznivé dopady zásahu na práva jednotlivců.[52]

49 Rozsudek ESLP ze dne 28. ledna 2003, *Peck v. Spojené království*, č. 44647/98, bod 85.

50 Rozsudek ESLP ze dne 26. března 1987, *Leander v. Švédsko*, č. 9248/81, bod 58.

51 Pracovní skupina pro ochranu údajů zřízená podle článku 29 (pracovní skupina zřízená podle článku 29) (2014), *Stanovisko k uplatňování pojmů nezbytnosti a proporcionality a ochrany údajů v oblasti vymáhání práva*, WP 211, Brusel, 27. února 2014, s. 7–8.

52 Tamtéž, s. 9–11.

Příklad: Ve věci *Khelili v. Švýcarsko*[53] policie během policejní kontroly zjistila, že stěžovatelka má u sebe navštívenky, na nichž je napsáno: „Milá, pohledná žena, zralá třicátnice, by ráda potkala muže, se kterým by občas popila nebo vyrazila do společnosti. Tel. č. […]". Stěžovatelka uváděla, že po tomto zjištění vložila policie její jméno do svých záznamů jako prostitutku. Že vykonává tuto profesi, však stěžovatelka soustavně popírala. Stěžovatelka požadovala, aby bylo slovo „prostitutka" vymazáno z policejních počítačových záznamů. ESLP v zásadě uznal, že uchovávání osobních údajů jednotlivce z toho důvodu, že by daná osoba mohla spáchat jiný trestný čin, může být za určitých okolností přiměřené. Avšak v případě stěžovatelky se nařčení z nezákonné prostituce jevila jako příliš vágní a obecná, nebyla podložena konkrétními fakty, protože stěžovatelka nikdy nebyla usvědčena z nezákonné prostituce, a nebylo proto možné se domnívat, že splňují podmínku „naléhavé společenské potřeby" ve smyslu článku 8 EÚLP. Soud se domníval, že je na orgánech, aby ověřily správnost uložených údajů o stěžovatelce a závažnost zásahu do jejích práv, a rozhodl, že zachování slova „prostitutka" v policejních spisech po řadu let nebylo nezbytné v demokratické společnosti. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci S. a Marper v. Spojené království[54] byli oba stěžovatelé zadrženi a obžalováni z trestných činů. Policie jim sejmula otisky prstů a odebrala vzorky DNA, jak stanoví Police and Criminal Evidence Act [zákon o policii a trestněprávním dokazování]. Stěžovatelé nikdy nebyli z těchto trestných činů usvědčeni: jednoho osvobodil soud a proti druhému stěžovateli bylo trestní stíhání zastaveno. Přesto byly jejich otisky prstů, profily DNA a vzorky buněčného materiálu uchovány a uloženy v policejní databázi a vnitrostátní právní předpisy povolily jejich uchovávání bez příslušné časové lhůty. Ačkoliv Spojené království namítalo, že uchovávání napomáhá při ztotožnění budoucích pachatelů, a tudíž sleduje legitimní cíl předcházení a odhalování trestné činnosti, ESLP zastával názor, že zásah do práva stěžovatelů na respektování jejich soukromého života byl neodůvodněný. Připomněl, že základní zásady ochrany údajů ukládají povinnost uchovávat osobní údaje přiměřeně s ohledem na účel shromažďování a že doba jejich uchovávání musí být omezena. Soud uznal, že rozšíření databáze tak, aby obsahovala profily DNA nejen odsouzených osob, ale také všech osob, které byly podezřívány, ale nebyly

53 Rozsudek ESLP ze dne 18. října 2011, *Khelili v. Švýcarsko*, č. 16188/07.

54 Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04.

odsouzeny, mohlo ve Spojeném království přispět k odhalování a předcházení trestné činnosti. Byl však „zaražen neomezenou a nevybíravou povahou pravomoci uchovávat údaje“.[55]

Vzhledem k tomu, jaké bohatství genetických informací a informací o zdraví je obsaženo ve vzorcích buněčné tkáně, byl zásah do práva stěžovatelů na soukromý život zvlášť rušivý. Otisky prstů a vzorky mohly být odebírány od zadržených osob a uchovávány neomezeně dlouhou dobu v policejních databázích bez ohledu na povahu nebo závažnost trestného činu, a to dokonce i v případech přestupků, které není možné trestat trestem odnětí svobody. Navíc možnosti osob zproštěných obvinění zajistit vymazání svých údajů z této databáze byly omezené. V neposlední řadě ESLP zvlášť přihlédl ke skutečnosti, že jednomu ze stěžovatelů bylo v době zatčení jedenáct let. Uchovávání osobních údajů nezletilých osob, které nejsou usvědčeny, může být zvlášť škodlivé vzhledem k jejich zranitelnosti a významu jejich vývoje a začlenění se do společnosti.[56] Soud jednomyslně rozhodl, že uchovávání představuje nepřiměřený zásah do práva na soukromý život, který nelze považovat za nezbytný v demokratické společnosti.

Příklad: Ve věci *Leander v. Švédsko*[57] ESLP rozhodl, že tajná prověrka osob ucházejících se o zaměstnání na pozicích významných pro národní bezpečnost není sama o sobě v rozporu s požadavkem na nezbytnost v demokratické společnosti. Zvláštní záruky stanovené ve vnitrostátním právu na ochranu zájmů subjektu údajů – například kontroly prováděné parlamentem a ministrem spravedlnosti – vedly ESLP k závěru, že švédský systém kontroly personálu splňoval požadavky stanovené v čl. 8 odst. 2 EÚLP. Vzhledem k širokému prostoru pro vlastní uvážení, který měl napadený stát k dispozici, byl oprávněn dospět k závěru, že v případě daného stěžovatele převažují zájmy národní bezpečnosti nad zájmy jednotlivce. Soud proto rozhodl, že nedošlo k porušení článku 8 EÚLP.

55 Tamtéž, bod 119.

56 Tamtéž, bod 124.

57 Rozsudek ESLP ze dne 26. března 1987, *Leander v. Švédsko*, č. 9248/81, body 59 a 67.

1.2.2. Podmínky pro zákonná omezení podle Listiny základních práv EU

Struktura a formulace Listiny a EÚLP se liší. Listina nepoužívá pojem zásahů do zaručených práv, ale obsahuje ustanovení o omezení(ch) výkonu práv a svobod uznaných Listinou.

Podle čl. 52 odst. 1 jsou omezení výkonu práv a svobod uznaných Listinou – a obdobně omezení výkonu práva na ochranu osobních údajů – přípustná pouze tehdy, pokud:

- jsou stanovena zákonem a
- respektují podstatu práva na ochranu údajů a
- jsou nezbytná s ohledem na zásadu proporcionality[58] a
- odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

Jelikož je v právním řádu EU ochrana osobních údajů odlišné a samostatné základní právo chráněné článkem 8 Listiny, veškeré zpracování osobních údajů jako takové představuje zásah do tohoto práva. Není podstatné, zda se dotčené osobní údaje týkají soukromého života jednotlivce, jsou citlivé nebo zda byly subjekty údajů jakýmkoliv způsobem uvedeny do nepříznivé situace. Má-li být zásah zákonný, musí být v souladu se všemi podmínkami uvedenými v čl. 52 odst. 1 Listiny.

Stanoveno zákonem

Omezení práva na ochranu osobních údajů musí být stanovena zákonem. Z tohoto požadavku vyplývá, že omezení musí mít právní základ, který je dostatečně přístupný a předvídatelný a který je formulován dostatečně přesně tak, aby umožnil jednotlivcům porozumět jejich závazkům a upravit jejich jednání. Právní základ musí též jasně definovat oblast působnosti a způsob výkonu pravomocí příslušnými orgány s cílem chránit jednotlivce před svévolnými zásahy. Tento výklad se podobá

58 Pro informace o posuzování nezbytnosti opatření omezujících základní právo na ochranu osobních údajů viz: EIOÚ (2017), *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*, Brusel, 11. dubna 2017.

požadavků na „zákonný zásah" podle judikatury ESLP[59] a má se za to, že význam výrazu „stanoveno zákonem", který je použit v Listině, by měl být shodný s významem, který je tomuto výrazu připisován v souvislosti s EÚLP.[60] Judikatura ESLP, a zejména pojem „kvalita zákona", který byl v judikatuře v průběhu let rozvíjen, jsou relevantním aspektem, který musí SDEU vzít v potaz při výkladu oblasti působnosti čl. 52 odst. 1 Listiny.[61]

Respektuje podstatu tohoto práva

V právním systému EU musejí veškerá omezení základních práv chráněných Listinou respektovat podstatu těchto práv. To znamená, že nelze odůvodnit omezení, která jsou natolik rozsáhlá a rušivá, že zbavují základní právo svého základního obsahu. Pokud je narušena podstata práva, musí být omezení považováno za protiprávní, aniž je nutné dále posuzovat, zda slouží cíli obecného zájmu a splňuje kritéria nezbytnosti a přiměřenosti.

Příklad: Ve věci *Schrems*[62] šlo o ochranu jednotlivců s ohledem na předávání jejich osobních údajů do třetích zemí – v dané věci do Spojených států. Rakouský občan Schrems, který byl několik let uživatelem Facebooku, podal stížnost u irského dozorového úřadu pro ochranu údajů, v níž odsoudil předávání svých osobních údajů z irské pobočky Facebooku společnosti Facebook Inc. a serverům umístěným v USA, kde byly zpracovány. Namítal, že s ohledem na odhalení, která v roce 2013 učinil Edward Snowden, americký whistleblower, týkající se činností sledování ze strany sledovacích služeb USA, nenabízí právo a praxe v USA dostatečnou ochranu osobních údajů předaných na území USA. Snowden odhalil, že se National Security Agency [Agentura pro národní bezpečnost] nabourala přímo do serverů firem, jako je Facebook, a mohla číst obsah komunikace a soukromých zpráv.

59 EIOÚ (2017), *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*, Brusel, 11. dubna 2017, s. 4; viz také SDEU, *Posudek 1/15 Soudního dvora (velkého senátu)*, 26. července 2017.

60 SDEU, spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* a *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, *Stanovisko generálního advokáta Saugmandsgaarda Øe*, přednesené dne 19. července 2016, bod 140.

61 SDEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM)*, *Stanovisko generálního advokáta Cruze Villalóna*, přednesené dne 14. dubna 2011, bod 100.

62 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

Předávání osobních údajů do USA bylo založeno na rozhodnutí Komise o odpovídající ochraně, které bylo přijato v roce 2000 a umožňovalo předávání údajů společnostem v USA, které samy osvědčily, že budou chránit osobní údaje předávané z EU a že budou jednat v souladu s takzvanými zásadami „bezpečného přístavu". Když byla věc předložena SDEU, soud přezkoumal platnost rozhodnutí Komise ve vztahu k Listině. Připomněl, že ochrana základních práv v EU vyžaduje, aby výjimky z těchto práv a jejich omezení byly činěny pouze v mezích toho, co je naprosto nezbytné. SDEU považoval právní úpravu, která veřejným orgánům umožňuje všeobecný přístup k obsahu elektronických komunikací, za „zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny". Právo by bylo zbaveno veškeré podstaty, kdyby orgány veřejné moci USA byly oprávněny k běžnému přístupu ke komunikacím bez jakéhokoli objektivního odůvodnění založeného na konkrétních důvodech národní bezpečnosti nebo předcházení trestným činům, které se konkrétně vážou k dotyčným osobám, a aniž by tyto praktiky v oblasti sledování byly doprovázeny odpovídajícími a ověřitelnými zárukami bránícími zneužití pravomocí.

Dále SDEU konstatoval, že „právní úprava, která nestanoví procesním subjektům žádnou možnost využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů", není slučitelná se základním právem na účinnou právní ochranu (článek 47 Listiny). Rozhodnutí o „bezpečném přístavu" tudíž nezajistilo úroveň ochrany základních práv ze strany USA, která by byla v zásadě rovnocenná úrovni zaručené v rámci EU podle směrnice ve spojení s Listinou. SDEU tedy rozhodnutí prohlásil za neplatné.[63]

Příklad: Ve věci *Digital Rights Ireland*[64] SDEU přezkoumal slučitelnost směrnice 2006/24/ES (směrnice o uchovávání údajů) se články 7 a 8 Listiny. Směrnice ukládala poskytovatelům služeb elektronických komunikací povinnost uchovávat provozní a lokační údaje po dobu nejméně šesti a nejvýše 24

63 Rozhodnutí SDEU o prohlášení neplatnosti rozhodnutí Komise 520/2000/ES bylo také podloženo jinými důvody, které budou přezkoumány v jiných oddílech této příručky. Zejména pak měl SDEU za to, že rozhodnutí protiprávně omezilo pravomoci vnitrostátních orgánů dozoru nad ochranou údajů. Kromě toho podle režimu „bezpečného přístavu" nebyly pro jednotlivce dostupné žádné soudní opravné prostředky v případě, že by chtěli získat přístup k osobním údajům, které se jich týkají, a/nebo dosáhnout jejich opravy nebo výmazu. Tím byla také narušena podstata základního práva na účinnou právní ochranu zakotvená v článku 47 Listiny.

64 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

měsíců a umožnit příslušným vnitrostátním orgánům přístup k těmto údajům za účelem prevence, vyšetřování, odhalování a stíhání závažných trestných činů. Směrnice neumožňovala uchovávání obsahu elektronických komunikací. SDEU konstatoval, že údaje, které poskytovatelé musejí uchovávat podle této směrnice, zahrnují údaje potřebné k dohledání a identifikaci zdroje a adresáta sdělení, datum, čas a dobu trvání komunikace, telefonní čísla volajícího a volaného a adresy internetového protokolu. Z těchto údajů „jako celku lze vyvodit velmi přesné závěry o soukromém životě osob, jejichž údaje byly uchovány, tedy o každodenních zvyklostech, o místech, kde trvale či přechodně pobývají, o denních či jiných přesunech, o jejich aktivitách, společenských vztazích těchto osob a o společenských kruzích, s kterými se stýkají".

Uchovávání osobních údajů podle této směrnice tudíž představovalo zvlášť závažný zásah do práv na soukromí a na ochranu osobních údajů. SDEU však dospěl k závěru, že zásah neměl nepříznivý dopad na podstatu těchto práv. Pokud jde o právo na soukromí, nebyla narušena podstata tohoto práva, protože tato směrnice neumožňuje seznámit se s obsahem elektronických sdělení jako takovým. Podobně nebyla narušena ani podstata práva na ochranu osobních údajů, protože směrnice stanoví, že poskytovatelé služeb elektronických komunikací musí dodržovat určité zásady ochrany a bezpečnosti údajů a že musí za tímto účelem přijmout vhodná technická a organizační opatření.

Nezbytnost a přiměřenost

Článek 52 odst. 1 Listiny stanoví, že při dodržení zásady proporcionality mohou být omezení výkonu základních práv a svobod uznaných Listinou zavedena pouze tehdy, pokud jsou nezbytná.

Omezení může být **nezbytné**, pokud je nutné přijmout opatření pro účely sledovaného cíle veřejného zájmu – ale nezbytnost podle výkladu SDEU také znamená, že přijatá opatření musejí být méně rušivá ve srovnávání s jinými možnostmi pro dosažení téhož cíle. U omezení práv na respektování soukromého života a ochrany osobních údajů SDEU používá zkoušku naprosté nezbytnosti, protože má za to, že „výjimky a omezení musí být činěny pouze v mezích toho, co je naprosto nezbytné". Pokud se omezení považuje za naprosto nezbytné, je také třeba posoudit, zda je přiměřené.

Přiměřeností se rozumí, že výhody vyplývající z omezení by měly převážit nad nevýhodami, které omezení způsobují, s ohledem na výkon dotčených základních práv.[65] V zájmu omezení nevýhod a rizik s ohledem na výkon práv na soukromí a ochranu údajů je důležité, aby omezení obsahovala vhodné záruky.

Příklad: Ve věci *Volker und Markus Schecke*[66] SDEU rozhodl, že tím, že vyžadují zveřejňování osobních údajů o každé fyzické osobě, která byla příjemcem podpory od některých zemědělských fondů, aniž činí rozdíl podle relevantních kritérií, jako je doba, po kterou tyto osoby takové podpory dostávaly, frekvence podpor nebo jejich typ a výše, překročily Rada a Komise omezení uložené zásadou proporcionality.

SDEU proto považoval za nezbytné prohlásit některá ustanovení nařízení Rady (ES) č. 1290/2005 za neplatná a nařízení č. 259/2008 prohlásil za neplatné v celém rozsahu.[67]

Příklad: Ve věci *Digital Rights Ireland*[68] SDEU rozhodl, že zásah do práva na soukromí způsobený směrnicí o uchovávání údajů nenarušil podstatu tohoto práva, protože směrnice zakazuje uchovávání obsahu elektronických komunikací. Dospěl však k závěru, že směrnice byla neslučitelná s článkem 7 a 8 Listiny, a prohlásil ji za neplatnou. Protože provozní a lokační údaje, ať už agregované, nebo pojímané jako celek, by mohly být analyzovány a vykreslit podrobný přehled o soukromém životě jednotlivců, jednalo se o závažný zásah do těchto práv. SDEU přihlédl k tomu, že směrnice vyžaduje uchovávání veškerých metadat o telefonii v rámci pevné sítě, mobilní telefonii, připojení k internetu, internetové elektronické poště a internetové telefonii, týká se použití všech prostředků elektronické komunikace – jejichž používání je velmi rozšířené v každodenním životě lidí. Představuje tedy zásah do základních práv téměř celé evropské populace. Vzhledem k rozsahu

65 EIOÚ (2017), *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*, s. 5.

66 Rozsudek SDEU (velkého senátu) ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, body 89 a 86.

67 Nařízení Rady (ES) č. 1290/2005 ze dne 21. června 2005 o financování společné zemědělské politiky, Úř. věst. 2005 L 209; nařízení Komise (ES) č. 259/2008 ze dne 18. března 2008, kterým se stanoví prováděcí pravidla k nařízení Rady (ES) č. 1290/2005, pokud jde o zveřejňování informací o příjemcích finančních prostředků z Evropského zemědělského záručního fondu (EZZF) a Evropského zemědělského fondu pro rozvoj venkova (EZFRV), Úř. věst. 2008 L 76.

68 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, bod 39.

a závažnosti tohoto zásahu lze uchovávání provozních a lokačních údajů podle SDEU odůvodnit pouze pro účely boje proti závažné trestné činnosti. Dále směrnice nestanovila žádná objektivní kritéria, která by zajistila, že přístup příslušných vnitrostátních orgánů k uchovávaným údajům se omezí pouze na rozsah, který je naprosto nezbytný. Kromě toho neobsahuje hmotněprávní a procesní podmínky pro přístup příslušných vnitrostátních orgánů k údajům a jejich využití, které nebylo podmíněno předchozím přezkumem ze strany soudu nebo jiného nezávislého orgánu.

SDEU dospěl k podobnému závěru ve spojených věcech *Tele2 Sverige AB v. Post- och telestyrelsen* a *Secretary of State for the Home Department v. Tom Watson a další*.[69] Tyto věci se týkaly uchovávání provozních a lokačních údajů „všech účastníků a registrovaných uživatelů a všech prostředků elektronické komunikace, ale také metadat" bez „rozlišování, omezení nebo výjimek podle sledovaného cíle".[70] V dané věci nebylo podmínkou pro uchovávání údajů to, zda je osoba spojena, ať už přímo, nebo nepřímo, se závažnými trestnými činy nebo zda mají její sdělení význam pro národní bezpečnost. Vzhledem k nepřítomnosti jednak nutné souvislosti mezi uchovávanými údaji a hrozbou pro veřejný pořádek, jednak omezení časové lhůty nebo zeměpisné oblasti SDEU dospěl k závěru, že vnitrostátní právní úprava překročila meze toho, co bylo naprosto nezbytné za účelem boje proti závažné trestné činnosti.[71]

Podobný přístup, pokud jde o nezbytnost, zaujal i evropský inspektor ochrany údajů ve svém *Necessity Toolkit* [Souboru nástrojů na posouzení nezbytnosti].[72] Cílem tohoto souboru nástrojů je pomoci posoudit soulad navrhovaných opatření s právem EU v oblasti ochrany údajů. Byl vypracován proto, aby poskytl lepší nástroje tvůrcům politik a normotvůrcům EU odpovědným za vypracování nebo kontrolu opatření, která zahrnují zpracování osobních údajů a omezují právo na ochranu osobních údajů a jiných práv a svobod stanovených v Listině.

69 Rozsudek SDEU (velkého senátu) ze dne 21. prosince 2016, spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och a Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, body 105–106.

70 Tamtéž, bod 105.

71 Tamtéž, bod 107.

72 EIOÚ (2017), *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*, Brusel, 11. dubna 2017.

Cíle obecného zájmu

Každé omezení výkonu práv uznaných Listinou, má-li být odůvodněné, musí také skutečně odpovídat cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého. Pokud jde o nutnost chránit práva a svobody druhého, právo na ochranu osobních údajů často interaguje s jinými základními právy. Oddíl 1.3 nabízí podrobnou analýzu těchto interakcí. Pokud jde o obecný zájem, patří sem obecné cíle EU stvrzené v článku 3 Smlouvy o Evropské unii (SEU), jako je podpora míru a blahobytu svých obyvatel, sociální spravedlnost a ochrana a vytvoření prostoru svobody, bezpečnosti a práva, v němž je zaručen volný pohyb osob, ve spojení s vhodnými opatřeními týkajícími se předcházení a potírání zločinnosti, jakož i jiné cíle a zájmy chráněné zvláštními ustanoveními smluv.[73] Obecné nařízení o ochraně osobních údajů dále upřesňuje čl. 52 odst. 1 Listiny takto: V čl. 23 odst. 1 nařízení je uveden seznam řady cílů obecného zájmu, které se považují za legitimní pro omezení práva jednotlivců, pokud omezení respektuje podstatu práva na ochranu osobních údajů a je nezbytné a přiměřené. K cílům veřejného zájmu uvedeným v tomto ustanovení patří národní bezpečnost a obrana, prevence trestných činů, ochrana důležitých hospodářských nebo finančních zájmů EU nebo členských států, veřejné zdraví a sociální zabezpečení.

Je důležité dostatečně podrobně definovat a vysvětlit cíl obecného zájmu, který dané omezení sleduje, protože nezbytnost omezení bude posuzována v kontextu tohoto cíle. Jasný, podrobný popis cíle omezení a navrhovaných opatření je zásadní k tomu, aby bylo možné provést posouzení nezbytnosti.[74] Sledovaný cíl a nezbytnost a přiměřenost omezení spolu úzce souvisí.

Příklad: Věc *Schwarz v. Stadt Bochum*[75] se týkala omezení práva na respektování soukromého života a práva na ochranu osobních údajů vyplývajících ze sejmutí a uchovávání otisků prstů při vydávání cestovních pasů orgány členských států.[76] Stěžovatel požádal město Bochum o vydání cestovního pasu, avšak odmítl, aby mu byly odebrány otisky prstů. Město Bochum jeho žádost následně zamítlo. Stěžovatel podal žalobu k německému soudu, v níž požadoval vydání cestovního pasu bez sejmutí otisků prstů. Německý soud

73 Vysvětlení k Listině základních práv (2007/C 303/02), Úř. věst. 2007 C 303, s. 17–35.

74 EIOÚ (2017), *Necessity Toolkit* [Soubor nástrojů na posouzení nezbytnosti], Brusel, 11. dubna 2017, s. 4.

75 Rozsudek SDEU ze dne 17. října 2013, C-291/12, *Michael Schwarz v. Stadt Bochum*.

76 Tamtéž, body 33–36.

postoupil věc SDEU a položil otázku, zda se považuje za platný čl. 1 odst. 2 nařízení (ES) č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy.

SDEU poukázal na to, že otisky prstů **představují osobní údaje**, neboť objektivně obsahují jedinečné informace o fyzických osobách a umožňují jejich přesnou identifikaci, zatímco snímání a ukládání otisků prstů představuje zpracování. Posledně uvedené zpracování, které se řídí čl. 1 odst. 2 nařízení (ES) č. 2252/2004, představuje zásah do práv na respektování soukromého života a ochranu osobních údajů.[77] Článek 52 odst. 1 Listiny však připouští omezení výkonu takových práv za předpokladu, že jsou tato omezení stanovena zákonem, respektují podstatu těchto práv a při dodržení zásady proporcionality jsou nezbytná a skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

Ve sporné věci SDEU nejprve konstatoval, že omezení, které vyplývá z odebrání a uchování otisků prstů v rámci vydání cestovního pasu, je třeba považovat za omezení **stanovené zákonem**, jelikož čl. 1 odst. 2 nařízení (ES) č. 2252/2004 tyto úkony stanoví. Dále má druhé uvedené nařízení bránit pozměňování cestovních pasů a jejich podvodnému použití. Článek 1 odst. 2 byl tudíž zaveden, aby bránil mimo jiné neoprávněnému vstupu do EU, a tudíž sleduje cíl obecného zájmu uznaný Unií. Zatřetí, ze skutečností, které měl SDEU k dispozici, nevyplývá a ostatně nebylo ani tvrzeno, že omezení kladená v projednávané věci na výkon práv nerespektují podstatu těchto práv. Začtvrté, uchování otisků prstů na vysoce zabezpečeném paměťovém médiu, jak stanoví dané opatření, vyžaduje pokročilou technologii. Toto uchování může snížit riziko pozměňování cestovních pasů a usnadnit úlohu orgánům, které mají na hranicích EU zkoumat pravost těchto cestovních pasů. Skutečnost, že metoda není zcela spolehlivá, není rozhodující. I když úplně nevylučuje přijetí všech neoprávněných osob, stačí, že významně snižuje pravděpodobnost takovýchto přijetí. S ohledem na výše uvedené úvahy SDEU konstatoval, že sejmutí a uchovávání otisků prstů podle čl. 1 odst. 2 nařízení (ES) č. 2252/2004 jsou způsobilá k dosažení cílů sledovaných tímto nařízením, a tudíž k dosažení cíle zabránit neoprávněnému vstupu osob na území EU.[78]

77 Tamtéž, body 27–30.

78 Tamtéž, body 35–45.

SDEU dále posuzoval, zda je takovéto zpracování **nezbytné**, a konstatoval, že napadený krok spočívá pouze v odebrání otisků dvou prstů, které navíc jiné osoby běžně vidí, takže se nejedná o úkon intimní povahy. Tento úkon není pro dotyčnou osobu ani zvláště fyzicky nebo psychicky nepříjemný, podobně jako pořízení zobrazení obličeje. Dále je třeba uvést, že jedinou skutečnou alternativou odebrání otisků prstů, která byla zmíněna v průběhu řízení před SDEU, je pořízení snímku oční duhovky. Nic ve spise předloženém SDEU však nenasvědčuje tomu, že by posledně uvedený postup zasahoval do práv přiznaných články 7 a 8 Listiny méně než odebrání otisků prstů. Pokud jde kromě toho o účinnost obou uvedených metod, je nesporné, že technologie rozpoznání oční duhovky není ještě natolik technologicky vyspělá jako metoda založená na otiscích prstů, je v současnosti podstatně dražší než srovnání otisků prstů, a tedy méně vhodná k obecnému používání. Soudní dvůr také nebyl seznámen s existencí opatření, která by mohla dostatečně účinně pomoci dosáhnout cíle ochrany cestovních pasů proti jejich podvodnému použití a zároveň by do práv přiznaných články 7 a 8 Listiny zasahovala méně než metoda založená na použití otisků prstů.[79]

SDEU konstatoval, že čl. 4 odst. 3 nařízení (ES) č. 2252/2004 výslovně uvádí, že otisky prstů mohou být použity pouze k ověření pravosti cestovního pasu a totožnosti jeho držitele, a současně čl. 1 odst. 2 uvedeného nařízení stanoví uchovávání otisků prstů pouze v samotném cestovním pase, který zůstává výlučně u svého držitele. Tudíž nařízení neposkytuje právní základ pro centralizované uchovávání údajů shromážděných na jeho základě nebo pro použití těchto údajů pro jiné účely, než je zabránit neoprávněnému vstupu osob na území EU.[80] S ohledem na veškeré výše uvedené úvahy SDEU dospěl k závěru, že přezkum položené otázky neodhalil žádnou skutečnost, kterou by mohla být dotčena platnost čl. 1 odst. 2 nařízení (ES) č. 2252/2004.

Vztah Listiny a EÚLP

I když jsou podmínky pro zákonná omezení práv formulovány odlišně, podmínky v čl. 52 odst. 1 Listiny připomínají podmínky v čl. 8 odst. 2 EÚLP týkající se práva na respektování soukromého života. Ve své judikatuře SDEU a ESLP často vzájemně odkazují na své rozsudky jako součást trvalého dialogu mezi oběma soudy při hledání harmonického výkladu pravidel v oblasti ochrany údajů. V čl. 52 odst. 3 Listiny

79 Rozsudek SDEU ze dne 17. října 2013, C-291/12, *Michael Schwarz v. Stadt Bochum*, body 46–53.

80 Tamtéž, body 56–61.

se uvádí: „Pokud tato listina obsahuje práva odpovídající právům zaručeným Úmluvou o ochraně lidských práv a základních svobod, jsou smysl a rozsah těchto práv stejné jako ty, které jim přikládá uvedená úmluva.“ Článek 8 Listiny však neodpovídá zcela článku EÚLP.[81] Článek 52 odst. 3 Listiny se týká rozsahu a oblasti působnosti práv chráněných jednotlivými právními řády, nikoliv podmínek pro jejich omezení. Avšak vzhledem k širšímu kontextu dialogu a spolupráce mezi oběma soudy může SDEU vzít v potaz ve svých analýzách kritéria pro zákonné omezení podle článku 8 EÚLP ve smyslu výkladu ESLP. Opačný scénář, kdy ESLP může odkazovat na podmínky pro zákonné omezení podle Listiny, je také možný. V každém případě je třeba také zohlednit, že v EÚLP neexistuje dokonalý ekvivalent článku 8 Listiny, který odkazuje na ochranu osobních údajů, a především pak na práva subjektu údajů, legitimní důvody pro zpracovávání a dozor ze strany nezávislého orgánu. Některé prvky článku 8 Listiny lze najít v judikatuře ESLP rozpracovávající článek 8 EÚLP a týkající se Úmluvy č. 108.[82] Tato souvislost zajišťuje existenci vzájemné inspirace mezi SDEU a ESLP ve věcech, které se týkají ochrany údajů.

1.3. Interakce s jinými právy a legitimními zájmy

Hlavní body

- Právo na ochranu osobních údajů často interaguje s jinými právy, například se svobodou projevu a právem přijímat a rozšiřovat informace.
- Tato interakce je často nejednoznačná: ačkoliv nastávají situace, kdy se právo na ochranu osobních údajů dostává do střetu s některým zvláštním právem, nastávají také situace, kdy právo na ochranu osobních údajů účinně zajišťuje dodržování téhož zvláštního práva. Je tomu tak například v případě svobody projevu, a to vzhledem k tomu, že služební tajemství je jednou složkou práva na respektování soukromého života.
- Nutnost chránit práva a svobody druhých je jedním z kritérií používaných pro posouzení zákonného omezení práva na ochranu soukromých údajů.
- Při konfliktu mezi různými právy musejí soudy provést jejich vyvážení ve snaze o uvedení těchto práv do vzájemného souladu.

81 EIOÚ (2017), *Necessity Toolkit* [Soubor nástrojů na posouzení nezbytnosti], Brusel, 11. dubna 2017, s. 6.

82 Vysvětlení k Listině základních práv (2007/C 303/02), článek 8.

- Obecné nařízení o ochraně osobních údajů ukládá členským státům povinnost uvést právo na ochranu osobních údajů do souladu se svobodou projevu a informací.
- Členské státy mohou také přijmout zvláštní pravidla ve vnitrostátním právu na uvedení práva na ochranu osobních údajů do souladu s přístupem veřejnosti k úředním dokumentům a s povinností zachovávat služební tajemství.

Právo na ochranu osobních údajů není právem absolutním – podmínky pro zákonné omezení byly podrobně rozebrány výše. Jedním z kritérií pro zákonná omezení práv, která přiznává právo RE i právo EU, je, aby zásah do ochrany údajů byl nezbytný pro ochranu práv a svobod druhých. Pokud ochrana údajů interaguje s jinými právy, ESLP i SDEU opakovaně konstatovaly, že při uplatňování a výkladu článku 8 EÚLP a článku 8 Listiny je nezbytné vyvážení s jinými právy.[83] Jak se tohoto vyvážení dosahuje, osvětlí několik významných příkladů.

Kromě vyvažování prováděného těmito soudy mohou státy, je-li to nutné, přijmout právní předpisy na uvedení práva na ochranu osobních údajů do souladu s jinými právy. Z tohoto důvodu stanoví obecné nařízení o ochraně osobních údajů řadu oblastí, kde mohou státy uplatňovat odchylky.

Pokud jde o svobodu projevu, ukládá nařízení GDPR členským státům povinnost uvést pomocí právních předpisů „právo na ochranu osobních údajů podle tohoto nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu“.[84] Členské státy také mohou přijmout právní předpisy na uvedení ochrany údajů do souladu s přístupem veřejnosti k úředním dokumentům a povinností zachovávat služební tajemství chráněné jako forma práva na respektování soukromého života.[85]

1.3.1. Svoboda projevu

Jedním z práv, které nejvýznamněji interaguje s právem na ochranu osobních údajů, je právo na svobodu projevu.

83 Rozsudek ESLP (velkého senátu) ze dne 7. února 2012, *Von Hannover v. Německo (č. 2)*, č. 40660/08 a 60641/08; rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, bod 48; rozsudek SDEU (velkého senátu) ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, bod 68.

84 Obecné nařízení o ochraně osobních údajů, článek 85.

85 Tamtéž, článek 86 a 90.

Svoboda projevu je chráněna článkem 11 Listiny („Svoboda projevu a informací"). Toto právo zahrnuje „svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice". Svoboda informací podle článku 11 Listiny i článku 10 EÚLP chrání právo nejen rozšiřovat, ale také *přijímat* informace.

Omezení svobody projevu musí být v souladu s kritérii uvedenými v čl. 52 odst. 1 Listiny, která jsou uvedena výše. Navíc článek 11 odpovídá článku 10 EÚLP. Podle čl. 52 odst. 3 Listiny platí, že pokud tato listina obsahuje práva odpovídající právům zaručeným EÚLP, „jsou smysl a rozsah těchto práv stejné jako ty, které jim přikládá uvedená úmluva". Omezení, která mohou být v souladu se zákonem uložena v případě práva zaručeného článkem 11 Listiny, proto nesmí jít nad rámec omezení, která jsou stanovena čl. 10 odst. 2 EÚLP – to znamená, že musí být stanovena zákonem a být nezbytná v demokratické společnosti „na ochranu pověsti nebo práv jiných". Tato práva zejména zahrnují právo na respektování soukromého života a právo na ochranu osobních údajů.

Vztah mezi ochranou osobních údajů a svobodou projevu upravuje článek 85 obecného nařízení o ochraně osobních údajů s názvem „Zpracování a svoboda projevu a informací". Podle tohoto článku mají členské státy povinnost uvést právo na ochranu osobních údajů do souladu s právem na svobodu projevu a informací. Zejména se stanoví výjimky a odchylky z jednotlivých kapitol obecného nařízení o ochraně osobních údajů pro novinářské účely a pro účely akademického, uměleckého či literárního projevu, pokud je to nutné k uvedení práva na ochranu osobních údajů do souladu se svobodou projevu a informací.

Příklad: Ve věci *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy a Satamedia Oy*[86] byl SDEU požádán, aby definoval vztah mezi ochranou údajů a svobodou tisku.[87] Musel přezkoumat šíření daňových údajů zhruba 1,2 milionu fyzických osob jistým podnikem prostřednictvím služby SMS. Tyto údaje byly získány legálně od finských daňových orgánů. Finský dozorový úřad pro ochranu údajů vydal rozhodnutí, kterým tomuto podniku uložil zastavit šíření těchto údajů. Podnik toto rozhodnutí napadl u vnitrostátního soudu,

86 Rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, body 56, 61 a 62.

87 Věc se týkala výkladu článku 9 směrnice o ochraně údajů – nyní nahrazen článkem 85 obecného nařízení o ochraně osobních údajů –, v němž se uvádí: „Členské státy stanoví pro zpracování osobních údajů prováděné výlučně pro účely žurnalistiky nebo uměleckého či literárního projevu, odchylky a výjimky z této kapitoly a z kapitol IV a VI, pouze pokud se ukáží jako nezbytné pro uvedení práva na soukromí do souladu s předpisy upravujícími svobodu projevu."

který požádal o objasnění SDEU, pokud jde o výklad směrnice o ochraně údajů. Zejména musel SDEU ověřit, zda zpracování osobních údajů, které daňové orgány zpřístupnily, aby umožnily uživatelům mobilních telefonů získávat daňové údaje týkající se jiných fyzických osob, je nutné považovat za činnost, která je vykonávána výlučně pro účely žurnalistiky. SDEU konstatoval, že činností podniku bylo „zpracování osobních údajů" ve smyslu čl. 3 odst. 1 směrnice o ochraně údajů, a následně analyzoval článek 9 směrnice (o zpracování osobních údajů a svobodě projevu). Nejprve konstatoval význam práva na svobodu projevu v každé demokratické společnosti a potvrdil, že pojmy týkající se této svobody, např. žurnalistiku, je třeba vykládat široce. Následně podotkl, že aby bylo dosaženo rovnováhy mezi oběma základními právy, musí být výjimky či omezení práva na ochranu údajů prováděny v mezích toho, co je naprosto nezbytné. Za těchto okolností SDEU konstatoval, že činnosti, jaké prováděly dané podniky, týkající se údajů pocházejících z dokumentů, které jsou podle vnitrostátních právních předpisů veřejné, mohou být kvalifikovány jako „činnosti žurnalistiky", jestliže je jejich účelem zpřístupnit veřejnosti informace, názory či myšlenky, ať již je způsob přenosu jakýkoli. Rozhodl také, že tyto činnosti nejsou vyhrazeny provozovatelům sdělovacích prostředků a mohou být spojeny s výdělečnými účely. SDEU však ponechal na vnitrostátním soudu, aby rozhodl, zda tomu tak bylo v daných skutkových okolnostech této věci.

Tutéž věc rovněž přezkoumal ESLP, a to po rozhodnutí vnitrostátního soudu, který na základě vodítka od SDEU konstatoval, že příkaz dozorového úřadu, aby bylo ukončeno zveřejňování všech daňových informací, byl oprávněným zásahem do svobody projevu této společnosti. I ESLP zastával tento přístup.[88] Dospěl k závěru, že i když došlo k zásahu do práva společnosti na rozšiřování informací, zásah byl v souladu se zákonem, sledoval legitimní cíl a byl nezbytný v demokratické společnosti.

Soud připomněl kritéria uvedená v judikatuře, která by měla být vodítkem pro vnitrostátní orgány a pro ESLP jako takový při vyvažování svobody projevu s právem na respektování soukromého života. Pokud jsou ohroženy politické projevy nebo debaty o záležitostech veřejného zájmu, existuje jen malý prostor pro omezování práva přijímat a rozšiřovat informace, protože veřejnost má právo být informována „a jedná se o nezbytné právo v demokratické

88 Rozsudek ESLP (velkého senátu) ze dne 27. června 2017, *Satakunnan Markkinapörssi Oy a Satamedia Oy v. Finsko*, č. 931/13.

společnosti“.[89] Za příspěvek k debatě ve veřejném zájmu však nelze považovat články v tisku, které mají za cíl pouze ukojit zvědavost konkrétní skupiny čtenářů, pokud jde o podrobnosti o soukromém životě dané osoby. Odchylka od pravidel na ochranu údajů pro novinářské účely má umožnit novinářům přístup k údajům, jejich shromažďování a zpracování tak, aby mohli provádět své žurnalistické činnosti. Proto skutečně existoval veřejný zájem na poskytování přístupu k dotčeným daňovým údajům a na umožnění podnikům, které jsou stěžovateli, velký objem těchto údajů shromažďovat a zpracovávat. Naproti tomu soud konstatoval, že neexistoval veřejný zájem na hromadném šíření těchto nezpracovaných údajů v novinách, v nezměněné podobě a bez jakékoliv analýzy. Informace o daních mohly umožnit zvědavým členům veřejnosti rozdělit osoby do kategorií podle jejich hospodářského postavení a uspokojit zájem veřejnosti o informace o soukromém životě druhých. To nelze považovat za příspěvek k debatě ve veřejném zájmu.

Příklad: Ve věci *Google Spain*[90] SDEU zvažoval, zda byla společnost Google povinna vymazat zastaralé informace o finančních potížích stěžovatele ze seznamu výsledků vyhledávání. Když byl do vyhledávače Googlu zadán dotaz pomocí jména stěžovatele, výsledky vyhledávání nabídly odkazy na staré novinové články, v nichž se uvádělo jeho spojení s insolvenčním řízením. Stěžovatel se domníval, že jde o porušení jeho práv na respektování soukromého života a na ochranu osobních údajů, protože řízení bylo uzavřeno před mnoha lety, a tudíž odkaz na ně byl irelevantní.

SDEU nejprve objasnil, že internetové vyhledávače a výsledky vyhledávání pomocí osobních údajů mohou vytvořit poměrně podrobný profil dané osoby. Vzhledem k tomu, že žijeme ve stále více digitalizované společnosti, je požadavek, aby osobní údaje byly správné a aby jejich zveřejňování nepřekračovalo rámec toho, co je nezbytné, tj. poskytování informací veřejnosti, zásadní k zajištění vysoké úrovně ochrany údajů pro jednotlivce. „Správce odpovědný za dané zpracování, v rámci své odpovědnosti, pravomoci a možností [musí] zajistit, aby toto zpracování splňovalo požadavky“ práva EU, mají-li mít stanovené právní záruky plný účinek. To znamená, že právo nechat vymazat vlastní osobní údaje, pokud jejich zpracování již není nezbytné nebo pokud jsou zastaralé, zahrnuje rovněž vyhledávače, o nichž bylo zjištěno, že jsou správci, nikoliv pouze zpracovateli (viz oddíl 2.3.1).

89 Tamtéž, bod 169.

90 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, body 81–83.

Při přezkumu, zda je společnost Google povinna odstranit odkazy související se stěžovatelem, SDEU konstatoval, že za určitých podmínek mají jednotlivci právo dosáhnout výmazu svých osobních údajů z výsledků vyhledávání internetových vyhledávačů. Na toto právo je možné se odvolat, pokud informace související s danou osobou jsou nesprávné, nedostatečné, irelevantní nebo nepřiměřeně rozsáhlé pro účely zpracování údajů. SDEU uznal, že toto právo není absolutní; je třeba je vyvážit s jinými právy, zejména zájmem a právem široké veřejnosti na přístup k informacím. Každá žádost o výmaz musí být posuzována individuálně, aby bylo dosaženo rovnováhy mezi základním právem na ochranu osobních údajů a na soukromý život subjektu údajů na straně jedné a mezi legitimními zájmy všech internetových uživatelů na straně druhé. SDEU poskytl vodítko k tomu, jaké prvky zvažovat během tohoto vyvažování. Zvlášť důležitým prvkem je povaha dotčené informace. Pokud je informace citlivá v souvislosti se soukromým životem jednotlivce a pokud neexistuje veřejný zájem na dostupnosti této informace, převáží ochrana údajů a soukromí nad právem široké veřejnosti získat k této informaci přístup. Naopak pokud se jeví, že subjekt údajů je veřejná osobnost nebo že tato informace je takové povahy, která odůvodňuje poskytnutí přístupu široké veřejnosti k této informaci, pak je zásah do základních práv na ochranu údajů a soukromí odůvodněný.

V návaznosti na rozsudek přijala pracovní skupina zřízená podle článku 29 pokyny k provádění tohoto rozsudku SDEU. Pokyny zahrnují seznam společných kritérií, která by měly orgány dozoru použít při vyřizování stížností týkajících se žádosti jednotlivce o výmaz a která by jim měla být vodítkem při vyvažování práv.[91]

Pokud jde o uvedení práva na ochranu osobních údajů do souladu s právem na svobodu projevu, ESLP vydal několik přelomových rozsudků.

91 Pracovní skupina zřízená podle článku 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 [Pokyny k provádění rozsudku SDEU ve věci „Google Spain a Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12]*, WP 225, Brusel, 26. listopadu 2014.

Příklad: Ve věci *Axel Springer AG v. Německo*[92] ESLP konstatoval, že zdržovací žaloba, která zabránila společnosti, která je stěžovatelem, zveřejnit článek o zatčení a usvědčení známého herce, je v rozporu s článkem 10 EÚLP. ESLP zopakoval kritéria, která se posuzují při vyvažování práva na svobodu projevu s právem na respektování soukromého života, jež jsou stanovena v jeho judikatuře:

- zda událost, jíž se zveřejněný článek týká, byla v obecném zájmu,
- zda daná osoba je veřejnou osobností a
- jak byly informace získány a zda jsou spolehlivé.

ESLP konstatoval, že hercovo zatčení a usvědčení bylo veřejným faktem u soudu, a proto bylo ve veřejném zájmu; že je herec dostatečně známý, aby jej bylo možné považovat za veřejnou osobnost; a že informace byly poskytnuty úřadem státního zástupce a jejich správnost žádná ze stran nezpochybňuje. Proto nebyla omezení uložená společnosti dostatečně přiměřená vzhledem k legitimnímu cíli, jímž bylo chránit soukromý život stěžovatele. Soud proto konstatoval, že došlo k porušení článku 10 EÚLP.

Příklad: Věc *Coudec a Hachette Filipacchi Associés v. Francie*[93] se týkala zveřejnění rozhovoru s paní Costeovou v jednom francouzském týdeníku. V tomto rozhovoru paní Costeová tvrdila, že otcem jejího syna je monacký kníže Albert. V rozhovoru se dále popisoval vztah paní Costeové s knížetem a způsob, jakým reagoval na narození dítěte, to vše bylo pak doplněno o fotografie knížete s dítětem. Kníže Albert zahájil řízení proti vydavatelské společnosti kvůli porušení svého práva na ochranu soukromého života. Francouzské soudy konstatovaly, že zveřejnění článku způsobilo knížeti Albertovi nenapravitelnou škodu, a nařídily vydavateli, aby zaplatil újmu a zveřejnil podrobnosti o rozsudku na přední obálce časopisu.

Vydavatelé časopisu předložili danou věci ESLP a tvrdili, že rozsudek francouzských soudů neoprávněně zasáhl do jejich práva na svobodu projevu. ESLP musel vyvážit právo knížete Alberta na respektování soukromého života

92 Rozsudek ESLP (velkého senátu) ze dne 7. února 2012, *Axel Springer AG v. Německo*, č. 39954/08, body 90 a 91.

93 Rozsudek ESLP (velkého senátu) ze dne 10. listopadu 2015, *Coudec a Hachette Filipacchi Associés v. Francie*, č. 40454/07.

s právem vydavatele na svobodu projevu a právem široké veřejnosti na získání informací. Významným hlediskem ke zvážení bylo také právo paní Costeové podělit se o svůj příběh s veřejností a zájem dítěte, aby byl oficiálně určen vztah otce a syna.

ESLP konstatoval, že zveřejnění rozhovoru představovalo zásah do soukromého života knížete, a dále přezkoumával, zda byl tento zásah nezbytný. Domníval se, že zveřejněné informace se týkají veřejné osobnosti a jsou záležitostí veřejného zájmu, protože občané Monaka mají zájem na tom dozvědět se o existenci dítěte knížete, protože budoucnost dědičné monarchie je „nedílně spjata s existencí potomků", a tudíž se jedná o záležitost, o kterou se veřejnost zajímá.[94] Soud také konstatoval, že článek umožnil paní Costeové a jejímu dítěti vykonávat své právo na svobodu projevu. Vnitrostátní soudy řádně nevzaly v potaz zásady a kritéria rozpracované v judikatuře ESLP za účelem vyvážení práva na respektování soukromého života a práva na svobodu projevu. Rozhodl, že Francie porušila článek 10 EÚLP týkající se svobody projevu.

V judikatuře ESLP je jedním z klíčových kritérií týkajících se vyvážení těchto práv to, zda daný projev přispívá k debatě v zájmu široké veřejnosti.

Příklad: Ve věci *Mosley v. Spojené království*[95] vnitrostátní týdeník zveřejnil intimní fotografie stěžovatele, známé osobnosti, která následně úspěšně zažalovala v občanskoprávním řízení vydavatele a byla jí přiznána náhrada škody. Navzdory přiznané peněžité náhradě škody si stěžoval, že je i nadále obětí porušování svého práva na soukromí, protože mu byla odepřena možnost podat zdržovací žalobu před zveřejněním dotčených fotografií, a to kvůli tomu, že neexistoval právní požadavek, aby noviny o zveřejnění předem informovaly.

ESLP konstatoval, že ačkoliv šíření takového materiálu probíhalo obecně za účelem pobavení, a nikoliv vzdělání, bezesporu požívá ochrany článku 10 EÚLP, který může ustoupit požadavkům článku 8 EÚLP, pokud byly informace soukromé a intimní povahy a na jejich šíření nebyl veřejný zájem. Je však třeba věnovat zvláštní péči přezkumu omezení, která mohou fungovat jako

94 Tamtéž, body 104–116.

95 Rozsudek ESLP ze dne 10. května 2011, *Mosley v. Spojené království*, č. 48009/08, body 129 a 130.

forma cenzury před samotným zveřejněním. S ohledem na odrazující účinek, který by takovýto požadavek na předběžné informování mohlo vyvolat, na pochybnosti o jeho účinnosti a na široký prostor pro vlastní uvážení v této oblasti ESLP rozhodl, že existence právně závazného požadavku na předběžné informování nebyla podle článku 8 nutná. Soud tudíž dospěl k závěru, že nedošlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Bohlen v. Německo*[96] stěžovatel, známý zpěvák a umělecký producent, zveřejnil autobiografickou knihu a následně byl donucen odstranit některé pasáže na základě soudního rozhodnutí. Událostí se intenzivně zabývaly vnitrostátní sdělovací prostředky a jistá tabáková společnost spustila humornou reklamní kampaň, ve které na tuto událost odkazuje a současně používá stěžovatelovo křestní jméno bez jeho souhlasu. Stěžovatel se neúspěšně domáhal náhrady škody od reklamní společnosti a odvolával se na porušení svých práv podle článku 8 EÚLP. ESLP zopakoval kritéria, která jsou vodítkem při nalézání rovnováhy mezi právem na respektování soukromého života a právem na svobodu projevu, a rozhodl, že nedošlo k porušení článku 8. Stěžovatel byl veřejně známá osobnost a reklama nepojednávala o podrobnostech z jeho soukromého života, ale o veřejné události, o které už informovaly sdělovací prostředky a která byla součástí veřejné diskuse. Kromě toho byla reklama humorné povahy a neobsahovala nic ponižujícího nebo negativního, pokud jde o stěžovatele.

Příklad: Ve věci *Biriuk v. Litva*[97] stěžovatelka před ESLP argumentovala, že Litva nesplnila svou povinnost zajistit respektování jejího práva na soukromý život, protože navzdory tomu, že jisté velké noviny závažně narušily jejího soukromí, přiřkly stěžovatelce vnitrostátní soudy šetřící tuto věc směšnou částku finančního odškodnění. Když vnitrostátní soudy určovaly odškodnění za jinou než finanční újmu, uplatnily ustanovení vnitrostátního práva o poskytování informací veřejnosti, které stanoví nízkou horní hranici pro odškodnění za jinou než finanční újmu způsobenou nezákonným předáním informací o soukromém životě dané osoby veřejnosti prostřednictvím sdělovacích prostředků. Věc se týkala toho, že největší litevský deník zveřejnil na titulní straně článek uvádějící, že stěžovatelka je HIV pozitivní. Článek také kritizoval stěžovatelčino chování a zpochybňoval její mravní normy.

96 Rozsudek ESLP ze dne 19. února 2015, *Bohlen v. Německo*, č. 53495/09, body 45–60.

97 Rozsudek ESLP ze dne 25. listopadu 2008, *Biriuk v. Litva*, č. 23373/03.

ESLP připomněl, že ochrana osobních údajů, a to i těch lékařských, má zásadní význam, pokud jde o právo na respektování soukromého života podle EÚLP. Důvěrnost zdravotních údajů je mimořádně důležitá, protože zveřejnění lékařských údajů (v tomto případě HIV status stěžovatelky) může zásadně ovlivnit soukromý a rodinný život dané osoby, její situaci v oblasti zaměstnání a její začlenění do společnosti. Soud přikládal mimořádný význam skutečnosti, že podle reportáže v novinách poskytli informace o stěžovatelčině HIV statusu zdravotničtí pracovníci v nemocnici, což je zjevné porušení jejich povinnosti zachovávat lékařské tajemství. Nedošlo tudíž k legitimnímu zásahu do stěžovatelčina práva na soukromý život.

Článek byl zveřejněn v tisku a svoboda projevu je také jedním ze základních práv podle EÚLP. Avšak při přezkumu, zda existence veřejného zájmu odůvodňovala zveřejnění tohoto druhu informací o stěžovatelce, soud rozhodl, že hlavním účelem zveřejnění bylo zvýšit prodej novin tím, že uspokojí zvědavost čtenářů. Není možné se domnívat, že by takovýto účel přispěl k jakékoliv diskusi v obecném zájmu společnosti. Jelikož v této věci došlo k „pobuřujícímu zneužití svobody tisku", značné omezení při nápravě újmy a nízká částka odškodnění za jinou než finanční újmu, kterou stanoví vnitrostátní právo, znamenaly, že Litva nesplnila svou pozitivní povinnost chránit právo stěžovatelky na soukromý život. ESLP proto shledal, že došlo k porušení článku 8 EÚLP.

Právo na svobodu projevu a právo na ochranu osobních údajů nejsou vždy v rozporu. Dochází k případům, kdy účinná ochrana soukromých údajů zaručuje svobodu projevu.

Příklad: SDEU ve věci *Tele2 Sverige* konstatoval, že zásah způsobený směrnicí 2006/24/ES (směrnice o uchovávání údajů) do základních práv stanovených v článcích 7 a 8 Listiny byl „rozsáhlý a musí být považován za zvlášť závažný. Okolnost, že k uchovávání údajů dochází bez vyrozumění uživatelů služeb elektronických komunikací, může v dotčených osobách vyvolávat dojem, že jejich soukromí je pod neustálým dohledem." SDEU rovněž konstatoval, že paušální uchovávání provozních a lokačních údajů by mohlo mít dopad na využívání elektronických komunikací a „v důsledku toho na výkon svobody projevu zaručené v článku 11 Listiny ze strany uživatelů těchto prostředků

komunikace“.[98] V tomto smyslu pravidla ochrany údajů tím, že požadují, aby přísné záruky pro uchovávání údajů nebyly prováděny paušálně, v konečném důsledku přispívají k výkonu svobody projevu.

Pokud jde o právo přijímat informace, které také tvoří součást svobody projevu, stále více si uvědomujeme význam transparentnosti vládnutí pro fungování demokratické společnosti. Transparentnost je jedním z cílů obecného zájmu, který by tudíž mohl odůvodnit zásah do práva na ochranu údajů, pokud je to nezbytné a přiměřené, jak je vysvětleno v oddíle 1.2. V uplynulých dvou desetiletích bylo tudíž uznáno právo na přístup k dokumentům v držení orgánů veřejné moci jako jedno z důležitých práv každého občana EU a každé fyzické nebo právnické osoby pobývající nebo usazené v některém členském státě.

Pokud jde o právo RE, je možné odkázat na zásady zakotvené v doporučení o přístupu k úředním dokumentům, které bylo inspirací pro vypracování Úmluvy o přístupu k úředním dokumentům (Úmluva č. 205).[99]

Pokud jde o právo EU, je právo na přístup k dokumentům zaručeno nařízením 1049/2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (nařízení o přístupu k dokumentům).[100] Článek 42 Listiny a čl. 15 odst. 3 SFEU rozšířily toto právo na přístup „k dokumentům orgánů, institucí a jiných subjektů Unie bez ohledu na jejich formu“.

Toto právo může kolidovat s právem na ochranu údajů, pokud by přístup k danému dokumentu současně odtajnil osobní údaje jiných osob. Článek 86 obecného nařízení o ochraně osobních údajů jasně stanoví, že osobní údaje v úředních dokumentech, které jsou v držení orgánu veřejné moci či veřejného nebo soukromého subjektu, může tento orgán či subjekt zpřístupnit v souladu s právem Unie[101] nebo členského

98 Rozsudek SDEU (velkého senátu) ze dne 21. prosince 2016, spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Tom Watson a další*, bod 101; rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, bod 28.

99 Rada Evropy, Výbor ministrů (2002), doporučení R (81) 19 a doporučení Rec(2002)2 členským státům o přístupu k úředním dokumentům, 21. února 2002; Rada Evropy, Úmluva o přístupu k úředním dokumentům, CETS č. 205, 18. června 2009. Úmluva dosud nevstoupila v platnost.

100 Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise, Úř. věst. 2001, L 145.

101 Článek 42 Listiny, čl. 15 odst. 3 SFEU a nařízení 1049/2009.

státu, aby tak zajistil soulad mezi přístupem veřejnosti k úředním dokumentům a právem na ochranu osobních údajů podle tohoto nařízení.

Je tedy možné, že u žádostí o přístup k dokumentům nebo informacím, které jsou v držení orgánů veřejné moci, bude třeba nalézt rovnováhu s právem na ochranu údajů osob, jejichž údaje jsou obsaženy v požadovaných dokumentech.

Příklad: Ve věci *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*[102] musel SDEU posoudit přiměřenost zveřejnění, jež požadují právní předpisy EU, pokud jde o jména příjemců zemědělských dotací EU a částky, které obdrželi. Zveřejnění mělo zvýšit transparentnost a přispět k veřejné kontrole použití veřejných prostředků ze strany správních orgánů. Přiměřenost tohoto zveřejnění napadlo několik příjemců.

SDEU konstatoval, že právo na ochranu osobních údajů není právem absolutním, a argumentoval, že zveřejnění údajů označujících příjemce dvou fondů zemědělské podpory EU a přesné výše obdržených částek na webové stránce představuje obecně zásah do jejich soukromého života a konkrétně pak do ochrany jejich osobních údajů.

SDEU konstatoval, že tento zásah do článků 7 a 8 Listiny byl stanoven zákonem a splňuje cíl obecného zájmu uznaného EU – konkrétně zvýšení transparentnosti využívání finančních prostředků Společenství. SDEU však měl za to, že zveřejnění jmen fyzických osob, které jsou příjemci zemědělské podpory EU z těchto dvou fondů, a přesné částky, kterou obdržely, představuje nepřiměřené opatření a není odůvodněné s ohledem na čl. 52 odst. 1 Listiny. Uznal význam toho, že v demokratické společnosti mají daňoví poplatníci právo být informováni o využívání veřejných prostředků. Avšak protože „cíli transparentnosti nelze přitom přiznat automatickou přednost před právem na ochranu osobních údajů“[103], jsou orgány EU povinny dosáhnout rovnováhy mezi zájmem Unie na transparentnosti a omezením výkonu práva na soukromí a práva na ochranu údajů, která příjemci utrpěli v důsledku zveřejnění.

102 Rozsudek SDEU (velkého senátu) ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, body 47–52, 58, 66–67, 75, 86 a 92.

103 Tamtéž, bod 85.

SDEU se domníval, že orgány EU nenalezly dostatečnou rovnováhu, protože bylo možné stanovit opatření, která by méně nepříznivě postihla základní práva jednotlivců a současně by také účinně přispěla k cíli transparentnosti, kterého se má zveřejněním dosáhnout. Například místo obecného zveřejňování, které by postihlo všechny příjemce, uvádělo jejich jména a přesnou výši částky, kterou každý z nich obdržel, je možné rozlišovat podle relevantních kritérií, jako je doba, po kterou takové podpory dostávali, frekvence podpor nebo jejich typ a výše.[104] SDEU tudíž prohlásil právní předpis EU o zveřejňování informací o příjemcích evropských zemědělských fondů za částečně neplatný.

Příklad: Ve věci *Rechnungshof v. Österreichischer Rundfunk a další*[105] SDEU přezkoumal slučitelnost jistého rakouského právního předpisu s právem EU na ochranu údajů. Tento právní předpis ukládal státnímu orgánu povinnost shromažďovat a sdělovat údaje o příjmech za účelem zveřejnění jmen a příjmů zaměstnanců různých veřejných subjektů ve výroční zprávě dostupné široké veřejnosti. Někteří jednotlivci odmítli sdělit své údaje z důvodu ochrany údajů.

Ve svém stanovisku SDEU vycházel z ochrany základních práv jako základní zásady práva EU a z článku 8 EÚLP a připomněl, že v té době nebyla Listina závazná. Konstatoval, že shromažďování údajů týkajících se profesních příjmů jednotlivce, zejména pak za účelem jejich sdělení třetím osobám, spadá do působnosti práva na respektování soukromého života a představuje porušení tohoto práva. Zásah by mohl být odůvodněný, pokud by byl v souladu se zákonem, sledoval by legitimní cíl a byl by nezbytný v demokratické společnosti, má-li být dosaženo tohoto cíle. SDEU konstatoval, že daný rakouský právní předpis sledoval legitimní cíl, protože jeho cílem bylo zachovat platy veřejných zaměstnanců v rozumných mezích – což je hledisko, které také souvisí s hospodářským blahobytem země. Avšak je třeba vyvážit zájem Rakouska na zajištění optimálního používání veřejných prostředků se závažností zásahu do práva na respektování soukromého života dotčených osob.

104 Tamtéž, bod 89.

105 Rozsudek SDEU ze dne 20. května 2003, spojené věci C-465/00, C-138/01 a C-139/01, *Rechnungshof v. Österreichischer Rundfunk a další a Christa Neukomm a Joseph Lauermann v. Österreichischer Rundfunk*.

SDEU přenechal předkládajícím soudům, aby ověřily, zda je zveřejňování údajů o příjmu jednotlivců nutné a přiměřené ve vztahu k cíli, který tento právní předpis sleduje, a současně vyzval vnitrostátní soudy, aby přezkoumaly, zda tohoto cíle nejde dosáhnout stejně účinně prostředky, které by méně narušovaly soukromí. Například by osobní údaje mohly být předávány pouze monitorovacím veřejným subjektům, a nikoliv široké veřejnosti.

V následujících věcech jasně vyplynulo, že rovnováha mezi ochranou údajů a přístupem k dokumentům vyžaduje podrobnou analýzu každého jednotlivého případu. Ani jedno právo nemůže být automaticky nadřazeno tomu druhému. SDEU dostal příležitost vyložit právo na přístup k dokumentům obsahujícím osobní údaje ve dvou věcech.

Příklad: Ve věci *Evropská komise v. Bavarian Lager*[106] SDEU definoval rozsah ochrany osobních údajů v souvislosti s přístupem k dokumentům orgánů EU a vztah mezi nařízením (ES) č. 1049/2001 (nařízení o přístupu k dokumentům) a nařízením (ES) č. 45/2001 (nařízení o ochraně údajů orgány EU). Společnost Bavarian Lager, založená v roce 1992, dováží stáčené německé pivo do Spojeného království, především do hostinců a barů. Potýkala se však s potížemi, protože britské právní předpisy *de facto* stanoví příznivější podmínky pro vnitrostátní výrobce. V reakci na stížnost společnosti Bavarian Lager Evropská komise zahájila řízení proti Spojenému království pro nesplnění jeho povinností, což Spojené království přimělo změnit sporná ustanovení a sladit je s právem EU. Společnost Bavarian Lager následně požádala Komisi kromě jiného o kopii zápisu ze zasedání, kterého se zúčastnili zástupci Komise, britské orgány a *Confédération des Brasseurs du Marché Commun* (CBMC). Komise souhlasila se zveřejněním některých dokumentů souvisejících s tímto zasedáním, ale zakryla pět jmen, která se v zápisu objevovala – dvě osoby výslovně vznesly námitku proti zveřejnění své totožnosti a Komise nedokázala získat kontakt na tři zbývající. Rozhodnutím ze dne 18. března 2004 Komise zamítla novou žádost společnosti Bavarian Lager o získání plné verze zápisu ze zasedání s odvoláním zejména na ochranu soukromého života těchto osob, kterou zaručuje nařízení o ochraně údajů orgány EU.

106 Rozsudek SDEU (velkého senátu) ze dne 29. června 2010, C-28/08 P, *Evropská komise v. The Bavarian Lager Co. Ltd.*

Protože Bavarian Lager nebyl s tímto postojem spokojen, podal žalobu k Soudu prvního stupně. Tento soud zrušil rozhodnutí Komise rozsudkem ze dne 8. listopadu 2007 (věc T-194/04, *The Bavarian Lager Co. Ltd v. Komise Evropských společenství*) a rozhodl, že pouhé zaznamenání jmen dotčených osob v seznamu osob, které se zúčastnily zasedání jménem subjektu, který zastupovaly, není narušením soukromého života a neuvádí soukromé životy těchto osob v nebezpečí.

Poté, co se Komise odvolala, SDEU zrušil rozsudek Soudu prvního stupně. SDEU konstatoval, že nařízení o přístupu k dokumentům zavádí „specifický a zesílený systém ochrany osob, jejichž osobní údaje mohou být případně zpřístupňovány veřejnosti". SDEU zastával názor, že pokud žádost na základě nařízení o přístupu k dokumentům usiluje o přístup k dokumentům obsahujícím osobní údaje, ustanovení nařízení o ochraně údajů orgány EU budou plně použitelná. SDEU pak vyvodil, že Komise správně zamítla žádost o přístup k úplnému znění zápisu ze zasedání z října 1996. Vzhledem k absenci souhlasu pěti účastníků tohoto zasedání bylo jednání Komise dostatečně v souladu s její povinností otevřenosti, protože zveřejnila verzi daného dokumentu se zakrytými jmény těchto osob.

Podle SDEU navíc „Komise – vzhledem k tomu, že Bavarian Lager nepředložila jakékoliv výslovné a legitimní odůvodnění ani žádný přesvědčivý argument k tomu, aby prokázala nutnost předání uvedených osobních údajů – nemohla poměřit jednotlivé zájmy dotčených osob. Nemohla ani ověřit, zda existují důvody domnívat se, že by takové předání mohlo poškodit legitimní zájmy subjektu údajů", jak to stanoví nařízení o ochraně údajů orgány EU.

Příklad: Ve věci *Client Earth a PAN Europe v. EFSA*[107] SDEU přezkoumal, zda rozhodnutí Evropského úřadu pro bezpečnost potravin (EFSA) odmítnout žadatelům plný přístup k dokumentům bylo nezbytné k ochraně práva na soukromí a na ochranu údajů osob, jichž se tyto dokumenty týkaly. Dokumenty pojednávaly o zprávě s návrhy pokynů o uvádění přípravků na ochranu rostlin na trh vypracované pracovní skupinou úřadu EFSA ve spolupráci s externími odborníky. Nejprve udělil úřad EFSA žadatelům přístup k části dokumentů a zamítl přístup k některým pracovním verzím dokumentu návrhu pokynů. Následně poskytl přístup k pracovní verzi, která obsahovala jednotlivé připomínky externích odborníků. Odstranil však jména odborníků s odvoláním na čl. 4 odst. 1 písm. b) nařízení (ES) č. 45/2001 o zpracování

107 Rozsudek SDEU ze dne 16. července 2015, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. Evropský úřad pro bezpečnost potravin (EFSA), Evropská komise*.

osobních údajů orgány a institucemi EU a na nutnost chránit soukromí externích odborníků. V prvním stupni Tribunál Evropské unie rozhodnutí úřadu EFSA potvrdil.

Poté, co žadatelé podali odvolání, SDEU rozsudek prvního stupně zvrátil. Dospěl k závěru, že předání osobních údajů bylo v daném případě nezbytné k ověření nestrannosti všech jednotlivých externích odborníků coby vědců při plnění jejich úkolů a k zajištění, aby proces rozhodování v úřadu EFSA byl i nadále transparentní. Podle SDEU úřad EFSA neupřesnil, jak by odtajnění jmen externích odborníků, kteří k dokumentu návrhu pokynů vznesli konkrétní připomínky, poškodilo legitimní zájmy těchto odborníků. Obecný argument, že zveřejnění by pravděpodobně narušilo soukromí, nepostačuje, pokud není podložen konkrétními důkazy pro každou jednotlivou věc.

Podle těchto rozsudků je u zásahů do práva na ochranu údajů v souvislosti s přístupem k dokumentům zapotřebí konkrétní a oprávněný důvod. Právo na přístup k dokumentům nemůže být automaticky nadřazeno právu na ochranu údajů.[108]

Tento přístup je podobný přístupu ESLP, pokud jde o soukromí a přístup k dokumentům, jak dokládá následující rozsudek. V rozsudku ve věci *Magyar Helsinki* ESLP konstatoval, že článek 10 neudílí jednotlivci právo na přístup k informacím v držení orgánu veřejné moci ani nezavazuje státní správu sdělovat tyto informace jednotlivci. Takovéto právo nebo povinnost by však mohla vzniknout – zaprvé pokud by zveřejnění těchto informací bylo uloženo soudním příkazem, který nabyl právní moci; zadruhé pokud by přístup k informacím pomohl jednotlivci při výkonu jeho práva na svobodu projevu – zvláště svobody přijímat a rozšiřovat informace – a pokud by odepření zasahovalo do tohoto práva.[109] Zda a v jaké míře odepření přístupu k informacím představuje zásah do svobody projevu žadatele, je třeba posoudit v každém jednotlivém případě a s ohledem na konkrétní okolnosti dané věci, včetně: i) účelu žádosti o informace; ii) druhu požadovaných informací; iii) úlohy žadatele a iv) zda byly informace připravené a dostupné.

108 Viz však podrobné úvahy EIOÚ (2011), *Public access to documents containing personal data after the Bavarian Lager ruling [Přístup veřejnosti k dokumentům obsahujícím osobní údaje po rozsudku ve věci Bavarian Lager]*, Brusel, 24. března 2011.

109 Rozsudek ESLP (velkého senátu) ze dne 8. listopadu 2016, *Magyar Helsinki Bizottság v. Maďarsko*, č. 18030/11, bod 148.

Příklad: Ve věci *Magyar Helsinki Bizottság v. Maďarsko*[110] stěžovatel, nevládní lidskoprávní organizace, požádala policii o informace týkající se činnosti obhájců *ex officio* s cílem vypracovat studii o fungování systému veřejných obhájců v Maďarsku. Policie tyto informace odmítla poskytnout a poukázala na to, že se jedná o osobní údaje, které nepodléhají zveřejnění. Za použití výše uvedených kritérií ESLP rozhodl, že došlo k zásahu do práva chráněného podle článku 10. Přesněji pak stěžovatel chtěl uplatňovat právo na rozšiřování informací o záležitosti ve veřejném zájmu, za tímto účelem žádal o přístup k informacím a informace byly nezbytné pro výkon stěžovatelova práva na svobodu projevu. Informace o přidělení veřejných obhájců byly v zájmu veřejnosti. Nebyl důvod pochybovat o tom, že dotčený průzkum obsahuje informace, které se stěžovatel snažil předat veřejnosti a které má veřejnost právo se dozvědět. Soud byl tedy uspokojen, že přístup k požadovaným informacím byl nezbytný k tomu, aby stěžovatel mohl plnit daný úkol. V neposlední řadě byly tyto informace připravené a dostupné.

ESLP konstatoval, že odepření přístupu k informacím v této věci narušilo samotnou podstatu svobody přijímat informace. Předtím, než dospěl k tomuto závěru, přezkoumal zejména účel požadovaných informací a jejich příspěvek k důležité veřejné diskusi, druh požadovaných informací a to, zda existuje veřejný zájem, a úlohu, již plní v dané věci ve společnosti stěžovatel.

Ve svém odůvodnění soud konstatoval, že studie vypracovaná touto nevládní organizací se týkala fungování spravedlnosti a práva na spravedlivé slyšení, které je v rámci EÚLP mimořádně důležitým právem. Jelikož se požadované informace netýkaly neveřejných údajů, nebylo by narušeno právo na soukromí dotčených subjektů údajů (veřejných obhájců *ex officio*), pokud by policie poskytla stěžovateli přístup k informacím. Informace, o které stěžovatel požádal, byly statistické povahy, týkaly se četnosti, s níž byli přidělováni obhájci *ex officio*, aby zastupovali obžalované ve veřejných trestních řízeních.

Soud se domníval, že vzhledem k tomu, že cílem studie bylo přispět k důležité diskusi o záležitosti v obecném zájmu, jakákoliv omezení týkající se publikace, již navrhla daná nevládní organizace, je třeba podrobit co nejpečlivějšímu přezkumu. Příslušné informace byly ve veřejném zájmu, protože veřejný zájem zahrnuje „záležitosti, které jsou schopné vyvolat značné kontroverze, které se týkají důležitého společenského problému nebo problému, o kterém

110 Tamtéž, body 181, 187–200.

by veřejnost ve vlastním zájmu měla být informována“.[111] Zahrnoval by tak jistě diskusi o vykonávání spravedlnosti a spravedlivém procesu, které jsou tématem stěžovatelovy studie. Po vyvážení jednotlivých dotčených práv a uplatnění zásady přiměřenosti ESLP rozhodl, že došlo k neodůvodněnému porušení práv stěžovatele podle článku 10 EÚLP.

1.3.2. Služební tajemství

Podle vnitrostátního práva mohou některá sdělení podléhat povinnosti zachovávat služební tajemství. Služební tajemství lze chápat jako zvláštní etickou povinnost, která je příčinou vzniku právního závazku u některých povolání a funkcí, které jsou založeny na důvěře. Osoby a instituce, které plní tyto funkce, jsou povinny nesdělovat důvěrné informace, které získaly při výkonu svých úkolů. Služební tajemství se vztahuje především na lékařské povolání a na výsadní vztah mezi advokátem a klientem, přičemž řada jurisdikcí rovněž uznává povinnost zachovávat služební tajemství ve finančním odvětví. Služební tajemství není základní právo, ale je chráněno jako jistá forma práva na respektování soukromého života. SDEU například v některých případech rozhodl, že „zákaz zveřejnit určité informace kvalifikované jako důvěrné skutečně může být nezbytný k tomu, aby bylo zachováno základní právo podniku na ochranu soukromého života, které je zakotvené v článku 8 EÚLP a v článku 7 Listiny“.[112] ESLP byl také vyzván, aby rozhodl, zda omezení služebního tajemství představují porušení článku 8 EÚLP, jak je ilustrováno ve vybraných příkladech.

Příklad: Ve věci *Pruteanu v. Rumunsko*[113] stěžovatel působil jako právník obchodní společnosti, které bylo zakázáno provádět bankovní transakce v návaznosti na obvinění z podvodu. Během šetření dané věci rumunské soudy povolily orgánům pověřeným stíháním po jistou dobu odposlouchávat a zaznamenávat telefonické rozhovory jednoho ze společníků. Součástí záznamů a odposlechů byly i rozhovory s jeho právníkem.

111 Tamtéž, bod 156.

112 Rozsudek SDEU ze dne 11. března 2013, věc T-462/12 R, *Pilkington Group Ltd v. Evropská komise*, usnesení předsedy Tribunálu, bod 44.

113 Rozsudek ESLP ze dne 3. února 2015, *Pruteanu v. Rumunsko*, č. 30181/05.

Pan Pruteanu namítal, že tento postup zasáhl do jeho práva na respektování soukromého života a korespondence. Ve svém rozsudku ESLP zdůraznil status a význam vztahu advokáta se svým klientem. Odposlouchávání rozhovoru advokáta s jeho klientem nepochybně narušilo služební tajemství, které bylo základem vztahu mezi těmito dvěma osobami. V takovém případě by si advokát také mohl stěžovat na zásah do svého práva na respektování soukromého života a korespondence. ESLP rozhodl, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Brito Ferrinho Bexiga Villa-Nova v. Portugalsko*[114] stěžovatelka, sama advokátka, odmítla zveřejnit výpis ze svého osobního účtu daňovým orgánům z důvodu profesní mlčenlivosti a bankovního tajemství. Úřad státního zástupce zahájil vyšetřování kvůli daňovému podvodu a požádal o povolení pozastavit povinnost zachovávat profesní mlčenlivost. Vnitrostátní soudy nařídily pozastavit povinnost zachovávat mlčenlivost a pravidla související s bankovním tajemstvím, protože dospěly k závěru, že by veřejný zájem měl převážit nad soukromými zájmy stěžovatelky.

Když byla věc předložena ESLP, soud konstatoval, že přístup k výpisu ze stěžovatelčina účtu představuje zásah do jejího práva na respektování služebního tajemství, které spadá do působnosti pojmu soukromý život. Zásah měl právní základ, protože byl založen na trestním zákoníku, a sledoval legitimní cíl. Avšak po přezkumu nezbytnosti a přiměřenosti zásahu ESLP poukázal na skutečnost, že řízení za účelem pozastavení tajemství byla provedena bez stěžovatelčiny účasti a bez jejího vědomí. Stěžovatelka tak nemohla předložit své argumenty. Kromě toho, i když vnitrostátní právo stanoví, že v takových řízeních je třeba konzultovat sdružení advokátů, toto sdružení konzultováno nebylo. V neposlední řadě pak stěžovatelka neměla možnost účinně napadnout zrušení povinnosti zachovávat mlčenlivost ani podat opravný prostředek, kterým by toto opatření napadla. Kvůli nedostatečným procesním zárukám a neúčinné soudní kontrole nad opatřením pozastavujícím povinnost zachovávat mlčenlivost dospěl ESLP k závěru, že došlo k porušení článku 8 EÚLP.

Interakce mezi povinností zachovávat služební tajemství a ochranou osobních údajů je často nejednoznačná. Pravidla a záruky týkající se ochrany údajů na jedné straně pomáhají zajišťovat služební tajemství. Například plavidla, která ukládají správcům

114 Rozsudek ESLP ze dne 1. prosince 2015, *Brito Ferrinho Bexiga Villa-Nova v. Portugalsko*, č. 69436/10.

a zpracovatelům provést solidní opatření v oblasti zabezpečení údajů, mají zabránit kromě jiného ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím. Kromě toho obecné nařízení EU o ochraně osobních údajů umožňuje zpracovávání údajů o zdravotním stavu, které představují zvláštní kategorii osobních údajů, jež vyžadují silnější ochranu, ale podmiňuje toto zpracování vhodnými a zvláštními opatřeními na zaručení práv subjektů údajů, zejména služebním tajemstvím.[115]

Na druhé straně povinnost zachovávat služební tajemství uložená správcům a zpracovatelům, pokud jde o některé osobní údaje, může omezit práva subjektů údajů, zejména právo přijímat informace. I když obecné nařízení o ochraně osobních údajů obsahuje úplný výčet informací, které v zásadě musí být subjektu údajů poskytnuty, pokud tyto osobní údaje nebyly získány od této osoby, tato povinnost sdělit informace neplatí, pokud osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu.[116]

Obecné nařízení o ochraně osobních údajů (GDPR) stanoví, že členské státy mohou právním předpisem přijmout zvláštní pravidla pro zajištění povinnosti zachovávat služební nebo jiné rovnocenné tajemství a uvést právo na ochranu osobních údajů do souladu s povinností zachovávat služební tajemství.[117]

GDPR stanoví, že členské státy mohou přijmout zvláštní pravidla týkající se pravomocí dozorových úřadů vůči správcům a zpracovatelům, kteří podléhají povinnosti zachovávat služební tajemství. Tato zvláštní pravidla se týkají pravomoci získat přístup do prostor správce nebo zpracovatele, k zařízení určenému ke zpracování údajů a osobním údajům, které spravuje, pokud tyto osobní údaje byly získány při činnosti, na niž se vztahuje povinnost zachovávat mlčenlivost. Dozorové úřady pověřené ochranou údajů tudíž musí respektovat povinnost zachovávat služební tajemství, kterou jsou vázáni správci a zpracovatelé. Kromě toho podléhají samotní členové dozorových úřadů také povinnosti zachovávat služební tajemství během svého funkčního období a po jeho skončení. Při výkonu svých povinností se mohou členové a pracovníci dozorových úřadů dozvědět důvěrné informace. Článek 54 odst. 2 tohoto nařízení jasně stanoví, že mají povinnost zachovávat služební tajemství s ohledem na takovéto důvěrné informace.

115 Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. h) a čl. 9 odst. 3.

116 Tamtéž, čl. 14 odst. 5 písm. d).

117 Tamtéž, 164. bod odůvodnění a článek 90.

GDPR členským státům ukládá povinnost informovat Komisi o pravidlech, která přijaly s cílem uvést ochranu osobních údajů a zásady stanovené v tomto nařízení do souladu s povinností zachovávat služební tajemství.

1.3.3. Svoboda náboženského vyznání nebo přesvědčení

Svoboda náboženského vyznání a přesvědčení je chráněna článkem 9 EÚLP (Svoboda myšlení, svědomí a náboženského vyznání) a článkem 10 Listiny základních práv EU. Osobní údaje, které odhalují náboženské nebo filozofické přesvědčení, se považují za „citlivé osobní údaje" podle práva EU i práva RE a jejich zpracování a využívání podléhá zvýšené ochraně.

Příklad: Stěžovatel ve věci *Sinan Işık v. Turecko*[118] byl členem náboženského společenství alevitů, jejichž víra je ovlivněna súfismem a jinými předislámskými náboženstvími a někteří vědci ji považují za samostatné náboženství a jiní za součást islámského náboženství. Stěžovatel si stěžoval, že proti jeho vůli obsahoval jeho občanský průkaz políčko uvádějící náboženství „islám", nikoliv „alevismus". Vnitrostátní soudy jeho žádost o změnu údaje v občanském průkazu na „alevismus" odmítly z důvodu, že toto slovo označuje podskupinu islámu, a nikoliv samostatné náboženství. Následně si stěžoval ESLP, že musel sdělit své náboženské přesvědčení, a to bez svého souhlasu, protože je povinné uvádět náboženství dané osoby na občanském průkazu, a že je tento postup v rozporu s jeho právem na svobodu náboženského vyznání a svědomí, zejména s ohledem na to, že označení „islám" na jeho občanském průkazu nebylo věcně správné.

ESLP zopakoval, že svoboda vyznání zahrnuje svobodu praktikovat své náboženské vyznání ve společnosti jiných, veřejně a v okruhu osob, které sdílí totéž vyznání, ale také v osamění a v soukromí. Vnitrostátní právní předpisy, které v té době platily, ukládaly jednotlivcům povinnost nosit u sebe občanský průkaz, což je dokument, kterým je třeba se na žádost jakéhokoliv orgánu veřejné moci nebo soukromého podniku legitimovat a na kterém je uvedeno náboženské vyznání dané osoby. Tato povinnost neuznávala, že právo praktikovat své náboženství platí i obráceně, tj. právo nemuset sdělovat své přesvědčení. Ačkoliv vláda namítla, že byl daný vnitrostátní předpis změněn, aby mohli jednotlivci požádat, aby políčko náboženství bylo

118 Rozsudek ESLP ze dne 2. února 2010, *Sinan Işık v. Turecko*, č. 21924/05.

v jejich občanských průkazech ponecháno prázdné, soud zastával názor, že samotná skutečnost, že je třeba žádat o vymazání náboženství, by mohla představovat sdělení informací o jejich postojích k náboženství. Kromě toho, pokud občanské průkazy mají políčko náboženství, zůstane-li takové políčko prázdné, vyvolává to zvláštní konotace, protože majitelé těchto průkazů bez informací o náboženství budou nápadní oproti těm, jejichž průkaz uvádí jejich vyznání. ESLP dospěl k závěru, že vnitrostátní právní předpisy jsou v rozporu s článkem 9 EÚLP.

Provoz církví a náboženských sdružení nebo společenství však může vyžadovat zpracovávání osobních informací členů s cílem umožnit komunikaci a organizaci činností v rámci kongregace. Církve a náboženská sdružení tudíž často zavádějí pravidla pro zpracovávání osobních údajů. Podle článku 91 obecného nařízení o ochraně osobních údajů, jestliže jsou tato pravidla komplexní, mohou nadále platit za předpokladu, že se uvedou do souladu s ustanoveními tohoto nařízení. Na církve a náboženská sdružení uplatňující takováto pravidla dohlíží nezávislý dozorový úřad, který může být zvláštní, za předpokladu, že splňuje podmínky stanovené v obecném nařízení o ochraně osobních údajů pro tyto úřady.[119]

Náboženská sdružení se mohou rozhodnout zpracovávat osobní údaje z několika důvodů – například za účelem zachování kontaktu se svou kongregací nebo za účelem předávání informací o náboženských a charitativních akcích a slavnostech, které se organizují. V některých státech musejí církve vést registry svých členů z důvodů daní, protože členství v náboženské obci může mít dopad na daně, které je jednotlivec povinen odvést. V každém případě podle evropského práva jsou údaje odhalující náboženské přesvědčení citlivými osobními údaji a církve musí nést odpovědnost za manipulaci s těmito údaji a jejich zpracovávání, a to zejména proto, že informace zpracovávané náboženskými organizacemi se často týkají dětí, starších lidí a jiných zranitelných členů společnosti.

1.3.4. Svoboda umění a věd

Dalším právem, které je třeba uvést do souladu s právy na respektování soukromého života a na ochranu údajů, je svoboda umění a věd, která je výslovně chráněna podle článku 13 Listiny základních práv EU. Toto právo je vyvozeno především z práva na svobodu myšlení a projevu a je třeba je uplatňovat s ohledem na článek 1 Listiny (Lidská důstojnost). ESLP považuje svobodu umění za chráněnou podle článku

119 Obecné nařízení o ochraně osobních údajů, čl. 91 odst. 2.

10 EÚLP.[120] Právo zaručené článkem 13 Listiny může také podléhat omezením podle čl. 52 odst. 1 Listiny, která lze též vykládat s přihlédnutím k čl. 10 odst. 2 EÚLP.[121]

Příklad: Ve věci *Vereinigung bildender Künstler v. Rakousko*[122] rakouské soudy zakázaly sdružení, které bylo stěžovatelem, nadále vystavovat obraz, který obsahoval fotografie hlav různých významných veřejných osobností v sexuálních polohách. Rakouský poslanec, jehož fotografie byla použita na obraze, zahájil řízení proti sdružení, které bylo stěžovatelem, a žádal o vydání soudního zákazu dalšího vystavování obrazu. Vnitrostátní soud takový zákaz vydal. ESLP zopakoval, že článek 10 EÚLP se vztahuje i na sdělování nápadů, které jsou urážlivé, šokující a rušivé pro stát nebo kteroukoliv část obyvatelstva. Osoby, které vytvářejí, předvádějí, distribuují nebo vystavují umělecká díla, přispívají k výměně myšlenek a názorů a stát má povinnost jejich svobodu projevu nepřiměřeně neomezovat. Vzhledem k tomu, že obraz byl koláží a použité fotografie zobrazovaly pouze hlavy osob, zatímco jejich těla byla namalována nerealisticky a přehnaně, což zjevně nemělo za cíl znázorňovat nebo i jen připomínat skutečnost, ESLP dále uvedl, že „obraz lze stěží chápat tak, že se týká podrobností ze soukromého života [znázorněné osoby], ale spíše tak, že se týká jeho veřejného postavení jakožto politika" a že „v této úloze [znázorněná osoba] musí prokázat větší toleranci, pokud jde o kritiku". ESLP zvážil různé zájmy, které byly dotčeny, a rozhodl, že neomezený zákaz dalšího vystavování obrazu je nepřiměřený. Soud proto shledal, že došlo k porušení článku 10 EÚLP.

Evropské právní předpisy o ochraně údajů rovněž uznávají zvláštní hodnotu vědy pro společnost. Obecné nařízení o ochraně osobních údajů a Modernizovaná úmluva č. 108 umožňují uchovávání údajů na delší dobu, pokud tyto osobní údaje budou zpracovány výlučně pro vědecké účely a účely historického výzkumu. Kromě toho a bez ohledu na původní účel činnosti zvláštního druhu zpracování se následné využití osobních údajů k vědeckému výzkumu nepovažuje za neslučitelný účel.[123] Zároveň však je nutné zavést dostatečné záruky pro takovéto zpracování s cílem ochránit práva a svobody subjektů údajů. Právo EU nebo členských států může stanovit

120 Rozsudek ESLP ze dne 24. května 1988, *Müller a další v. Švýcarsko*, č. 10737/84.

121 Vysvětlení k Listině základních práv, Úř. věst. 2007 C 303.

122 Rozsudek ESLP ze dne 25. ledna 2007, *Vereinigung bildender Künstler v. Rakousko*, č. 68345/01, body 26 a 34.

123 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. b) a Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b).

odchylky z práv subjektů údajů, jako například právo na přístup, opravu, omezení zpracování a právo vznést námitku, pokud jde o zpracování osobních údajů pro účely vědeckého výzkumu, historické nebo statistické účely (viz též oddíl 6.1 a oddíl 9.4).

1.3.5. Ochrana duševního vlastnictví

Právo na ochranu vlastnictví je zakotveno v článku 1 prvního protokolu k EÚLP a také v čl. 17 odst. 1 Listiny základních práv EU. Jedním významným aspektem práva na vlastnictví, které je zvlášť významné pro ochranu údajů, je ochrana duševního vlastnictví, jež je výslovně uvedena v čl. 17 odst. 2 Listiny. Účinná ochrana duševního vlastnictví a zejména autorského práva je pak cílem několika směrnic v právním řádu EU. Duševní vlastnictví zahrnuje nejen literární a umělecké vlastnictví, ale také patenty, ochranné známky a související práva.

Jak bylo objasněno v judikatuře SDEU, ochrana základního práva na vlastnictví musí být sladěna s ochranou jiných základních práv, zejména práva na ochranu údajů.[124] Došlo k případům, kdy instituce zabývající se ochranou autorského práva požadovaly, aby jim poskytovatelé přístupu k internetu sdělili totožnost uživatelů platforem pro sdílení souborů. Tyto platformy často internetovým uživatelům umožňují stáhnout si hudební tituly zdarma, ačkoliv jsou chráněny autorským právem.

Příklad: Věc *Promusicae v. Telefónica de España*[125] se týkala toho, že španělský poskytovatel přístupu k internetu, společnost Telefónica, odmítla zpřístupnit neziskové organizaci hudebních producentů a vydavatelství hudebních a audiovizuálních nahrávek Promusicae osobní údaje některých osob, jimž poskytla služby přístupu k internetu. Sdružení Promusicae chtělo, aby mu byly zpřístupněny informace, aby mohlo zahájit občanskoprávní řízení proti těmto osobám, které podle jeho tvrzení používaly program pro výměnu souborů, který umožňoval přístup ke zvukovým záznamům, k nimž práva dílo užít náležejí členům sdružení Promusicae.

Španělský soud postoupil věc SDEU a požádal jej, zda takovéto osobní údaje musí být podle práva Společenství zpřístupněny v rámci občanskoprávního řízení s cílem zajistit účinnou ochranu autorského práva. Poukázal na směrnice 2000/31/ES, 2001/29/ES a 2004/48/ES též ve spojení s články 17 a 47

124 Rozsudek SDEU (velkého senátu) ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, body 62–68.

125 Tamtéž, body 54 a 60.

Listiny. SDEU dospěl k závěru, že tyto tři směrnice a ani směrnice o soukromí a elektronických komunikacích (směrnice 2002/58/ES) nevylučují možnost, aby členské státy stanovily povinnost zpřístupnit osobní údaje v rámci občanskoprávního řízení, a zajistily tak účinnou ochranu autorského práva.

SDEU poukázal na to, že ve věci proto vyvstává otázka nutného vyvážení požadavků spojených s ochranou různých základních práv – totiž práva na respektování soukromého života a práva na ochranu vlastnictví i práva na účinnou právní ochranu.

Dospěl k závěru, že „členské státy musejí při provádění výše uvedených směrnic dbát na to, aby se opíraly o výklad těchto směrnic, který umožní zajistit spravedlivou rovnováhu mezi jednotlivými základními právy chráněnými právním řádem Společenství. Dále je nutné, aby při plnění opatření, která tyto směrnice provedly ve vnitrostátním právním řádu, orgány a soudy členských států nejen vykládaly své vnitrostátní právo v souladu s těmito směrnicemi, ale rovněž, aby se neopíraly o takový jejich výklad, který by byl v rozporu s danými základními právy nebo s jinými obecnými zásadami práva Společenství, jako je zásada přiměřenosti.“[126]

Příklad: Věc *Bonnier Audio AB a další v. Perfect Communication Sweden AB*[127] se týkala rovnováhy mezi právy duševního vlastnictví a ochranou osobních údajů. Stěžovatelé – pět vydavatelských společností, které jsou majiteli autorských práv k 27 audioknihám – zahájili řízení u švédského soudu a tvrdili, že tato autorská práva byla porušena prostřednictvím serveru FTP (protokol pro přenos souborů, který umožňuje sdílení souborů a přenášení dat přes internet). Stěžovatelé požadovali, aby poskytovatel internetových služeb sdělil jména a adresy osoby, která používá IP adresu, z níž jsou soubory odesílány. Poskytovatel internetových služeb, společnost ePhone, žalobu zpochybnila tvrzením, že je v rozporu se směrnicí 2006/24 (směrnice o uchovávání údajů – zrušena v roce 2014).

Švédský soud věc postoupil SDEU s otázkou, zda směrnice 2006/24 brání použití vnitrostátního ustanovení zavedeného na základě článku 8 směrnice 2004/48/ES (směrnice o dodržování práv duševního vlastnictví), které

126 Tamtéž, body 65 a 68; viz také rozsudek SDEU ze dne 16. února 2012, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*.

127 Rozsudek SDEU ze dne 19. dubna 2012, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*.

umožňuje vydat soudní příkaz ukládající poskytovateli internetových služeb povinnost předat majiteli autorského práva informace o účastnících, jejichž IP adresa byla údajně použita při porušení práva. Otázka vycházela z předpokladu, že stěžovatel uvedl jasný důkaz, že došlo k porušení konkrétního autorského práva a že opatření je přiměřené.

SDEU poukázal na to, že se směrnice 2006/24/ES vztahuje výlučně na zpracovávání a uchovávání údajů vytvářených nebo zpracovávaných poskytovateli veřejně dostupných služeb elektronických komunikací pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jakož i jejich poskytování příslušným vnitrostátním orgánům. Vnitrostátní ustanovení provádějící směrnici o dodržování práv duševního vlastnictví do vnitrostátního práva tudíž není v oblasti působnosti směrnice 2006/24/ES, a tato směrnice tudíž nebrání jeho uplatnění.[128]

Pokud jde o sdělení dotyčného jména a adresy, o které žádají stěžovatelé, SDEU rozhodl, že toto opatření představuje zpracovávání osobních údajů a spadá do působnosti směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích). Připomněl také, že sdělení těchto údajů bylo požadováno v rámci občanskoprávního řízení ve prospěch majitele autorského práva za účelem účinné ochrany autorského práva, a tudíž také patří svým předmětem do působnosti směrnice 2004/48/ES.[129]

SDEU dospěl k závěru, že směrnice 2002/58/ES a 2004/48/ES musí být vykládány v tom smyslu, že nebrání takové vnitrostátní právní úpravě, o jakou se jedná v původním řízení, v rozsahu, v němž tato právní úprava umožňuje vnitrostátnímu soudu, jemuž byl předložen návrh na vydání soudního příkazu ke sdělení osobních údajů, zvážit dotčené protichůdné zájmy v závislosti na okolnostech každého případu a s ohledem na požadavky vyplývající ze zásady proporcionality.

128 Tamtéž, body 40–41.

129 Tamtéž, body 52–54. Viz také rozsudek SDEU (velkého senátu) ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, bod 58.

1.3.6. Ochrana údajů a hospodářské zájmy

V digitálním věku nebo ve věku dat velkého objemu se data označují jako „nová ropa“ hospodářství, která podněcuje inovace a kreativitu.[130] Řada společností na zpracování dat vybudovala solidní obchodní modely a toto zpracování se často týká osobních údajů. Některé společnosti jsou možná přesvědčeny, že konkrétní pravidla týkající se ochrany osobních údajů mohou mít v praxi za následek nadměrně zatěžující povinnosti, které by mohly ovlivnit jejich hospodářské zájmy. Vyvstává tudíž otázka, zda by mohly odůvodnit omezení práva na ochranu údajů hospodářské zájmy správců a zpracovatelů nebo zájmy široké veřejnosti.

Příklad: Ve věci *Google Spain*[131] SDEU rozhodl, že za jistých podmínek mají jednotlivci právo požádat vyhledávače, aby odstranily výsledky vyhledávání ze svého indexu vyhledávání. Ve svém odůvodnění SDEU poukázal na skutečnost, že používání vyhledávačů a seznamů výsledků vyhledávání může vytvořit podrobný profil jednotlivce. Tyto informace se mohou týkat rozsáhlých aspektů soukromého života jednotlivce a bez vyhledávače by nebylo možné je snadno dohledat nebo vzájemně propojit. Jedná se tedy o potenciálně závažný zásah do základních práv subjektů údajů na soukromí a ochranu osobních údajů.

SDEU následně zkoumal, zda by mohl být zásah odůvodněný. Pokud jde o hospodářský zájem společnosti provozující vyhledávač na provádění zpracování, SDEU konstatoval, že „tento zásah nelze odůvodnit pouze hospodářským zájmem provozovatele vyhledávače na takovém zpracování“ a že „obecně“ základní práva podle článku 7 a 8 Listiny převažují nad takovýmto hospodářským zájmem a zájmem široké veřejnosti nalézt uvedenou informaci při vyhledávání prováděném na základě jména subjektu údajů.[132]

Jedním z klíčových aspektů evropského práva na ochranu údajů je poskytnout jednotlivcům větší kontrolu nad jejich osobními údaji. Zejména v digitálním věku panuje nerovnováha mezi pravomocemi podnikatelských subjektů, které zpracovávají a mají přístup k obrovskému objemu osobních údajů, a pravomocemi jednotlivců,

130 Viz například *Financial Times* (2016), „Data is the new oil… who's going to own it?“ [Data jsou nová ropa… kdo je bude vlastnit?], 16. listopadu 2016.

131 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

132 Tamtéž, body 81 a 97.

kterým tyto osobní údaje patří, své informace kontrolovat. SDEU zastává individuální přístup podle okolností jednotlivých případů, pokud jde o vyvážení ochrany údajů a hospodářských zájmů – jako jsou například zájmy třetích stran v souvislosti s akciovými společnostmi a společnostmi s ručením omezeným, jak dokládá rozsudek ve věci *Manni*.

Příklad: Věc *Manni*[133] se týkala vedení osobních údajů jednotlivce ve veřejném obchodním rejstříku. Pan Manni požádal obchodní komoru v Lecce, aby vymazala jeho osobní údaje z rejstříku poté, co zjistil, že případní zákazníci mohou nahlížet do rejstříku a zjistit, že byl jednatelem společnosti, která před více než deseti lety vyhlásila úpadek. Tato informace odrazovala případné zákazníky a mohla mít nepříznivý dopad na jeho obchodní zájmy.

SDEU byl vyzván, aby rozhodl, zda právo EU uznává v dané věci právo na výmaz. Ve svém závěru pak soud zvážil práva ochrany údajů EU a obchodní zájem pana Manniho na odstranění informací o úpadku jeho někdejší společnosti na jedné straně a veřejný zájem na přístup k informacím na straně druhé. Připomněl skutečnost, že toto zveřejnění informace ve veřejném rejstříku obchodních společností je stanoveno zákonem, a především směrnicí EU, která má za cíl usnadnit třetím osobám přístup k informacím o společnostech. Zveřejnění je důležité pro ochranu zájmů třetích osob, které mohou chtít obchodovat s danou společností, protože jediné záruky, které třetím osobám nabízí akciová společnost a společnost s ručením omezeným, jsou její aktiva. Proto „by zveřejňování mělo třetím osobám umožnit, aby se seznámily se základními listinami společnosti a s některými údaji, které se jí týkají, zejména s údaji o osobách, které jsou oprávněny společnost zavazovat".[134]

Vzhledem k významu legitimního cíle, který rejstřík sleduje, SDEU rozhodl, že pan Manni nemá právo dosáhnout výmazu svých osobních údajů, protože nad jeho právy podle právních předpisů o ochraně osobních údajů převažuje nezbytnost chránit zájmy třetích osob ve vztahu k akciovým společnostem a ke společnostem s ručením omezeným a zajistit právní jistotu, poctivost obchodních transakcí, a tedy i řádné fungování vnitřního trhu. Tento závěr

133 Rozsudek SDEU ze dne 9. března 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*.

134 Tamtéž, bod 49.

zvlášť potvrzuje skutečnost, že osoby, které se rozhodnou účastnit se obchodování prostřednictvím takové společnosti, si jsou vědomy, že musejí zveřejnit informace týkající se jejich totožnosti a jejich funkcí.

SDEU sice rozhodl, že nejsou v této věci žádné důvody pro dosažení výmazu, přesto však uznal existenci práva vznést námitku ke zpracování a konstatoval: „není možné vyloučit, že mohou existovat zvláštní situace, v nichž vážné a legitimní důvody související s konkrétní situací subjektu údajů výjimečně odůvodňují, aby byl po uplynutí dostatečně dlouhé doby […] omezen přístup k osobním údajům zapsaným v rejstříku […] ve vztahu ke třetím osobám, které prokáží zvláštní zájem na nahlížení do těchto údajů.“[135]

SDEU konstatoval, že je úkolem vnitrostátních soudů v každém jednotlivém případě posoudit s přihlédnutím ke všem relevantním okolnostem daného jednotlivce, zda existují nebo neexistují legitimní a převažující důvody, které by mohly výjimečně odůvodňovat omezení přístupu třetích osob k osobním údajům uvedeným v obchodních rejstřících. Vyjasnil však, že ve věci pana Manniho pouhá okolnost, že zveřejnění jeho osobních údajů v rejstříku údajně ovlivnilo jeho klientelu, nemůže být považována za takovýto legitimní a převažující důvod. Případní klienti pana Manniho mají legitimní zájem na informacích o úpadku jeho předchozí společnosti.

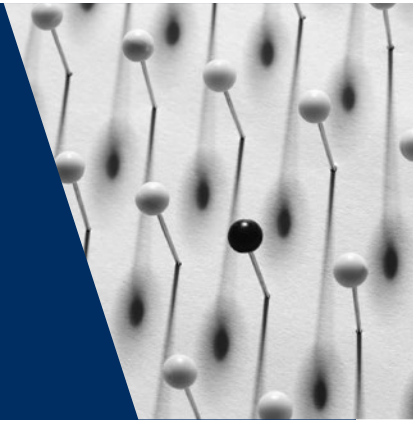
Zásah do základního práva pana Manniho a jiných osob uvedených v rejstříku na respektování soukromého života a na ochranu osobních údajů, jež jsou zaručeny článkem 7 a 8 Listiny, slouží cíli obecného zájmu a je nezbytný a přiměřený.

Ve věci *Manni* proto SDEU rozhodl, že práva na ochranu údajů a soukromí nepřevažují nad zájmem třetích osob mít přístup k informacím v rejstříku společností, pokud jde o akciové společnosti a společnosti s ručením omezeným.

135 Tamtéž, bod 60.

2

Terminologie v oblasti ochrany osobních údajů



EU	Pojednávaná témata	RE
Osobní údaje		
Obecné nařízení o ochraně osobních údajů, čl. 4 bod 1 Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 5 a čl. 5 odst. 1 písm. e) Obecné nařízení o ochraně osobních údajů, článek 9 Rozsudek SDEU (velkého senátu) z roku 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen* Rozsudek SDEU (velkého senátu) z roku 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* Rozsudek SDEU z roku 2011, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* Rozsudek SDEU z roku 2016, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland* Rozsudek SDEU z roku 2014, spojené věci C-141/12 a C-372/12, YS v. *Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M a S*	**Právní definice ochrany údajů**	Modernizovaná úmluva č. 108, čl. 2 písm. a) Rozsudek ESLP z roku 2013, *Bernh Larsen Holding AS a další v. Norsko*, č. 24117/08 Rozsudek ESLP z roku 2010, *Uzun v. Německo*, č. 35623/05 Rozsudek ESLP (velkého senátu) z roku 2000, *Amann v. Švýcarsko*, č. 27798/95

EU	Pojednávaná témata	RE
Rozsudek SDEU z roku 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*	**Zvláštní kategorie osobních údajů (citlivé osobní údaje)**	Modernizovaná úmluva č. 108, čl. 6 odst. 1
Rozsudek SDEU (velkého senátu) z roku 2017, C-434/16, *Peter Nowak v. Data Protection Commissioner*	**Anonymizované a pseudo-nymizované osobní údaje**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. e) Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 50
Zpracování údajů		
Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 2 Rozsudek SDEU z roku 2014, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů* Rozsudek SDEU z roku 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni* Rozsudek SDEU z roku 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist* Rozsudek SDEU (velkého senátu) z roku 2014, C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*	**Definice**	Modernizovaná úmluva č. 108, čl. 2 písm. b) a c)
Uživatelé údajů		
Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 7 Rozsudek SDEU z roku 2014, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů* Rozsudek SDEU (velkého senátu) z roku 2014, C-1318/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*	**Správce**	Modernizovaná úmluva č. 108, čl. 2 písm. d) Doporučení o profilování, čl. 1 písm. g)*
Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 8	**Zpracovatel**	Modernizovaná úmluva č. 108, čl. 2 písm. f) Doporučení o profilování, čl. 1 písm. h)
Obecné nařízení o ochraně osobních údajů, čl. 4 odst. 9	**Příjemce**	Modernizovaná úmluva č. 108, čl. 2 písm. e)
Obecné nařízení o ochraně osobních údajů, čl. 4 bod 10	**Třetí strana**	

EU	Pojednávaná témata	RE
Souhlas		
Obecné nařízení o ochraně osobních údajů, čl. 4 bod 11 a článek 7 Rozsudek SDEU z roku 2011, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland* Rozsudek SDEU z roku 2017, C-536/15, *Tele2 (Netherlands) BV a další v. Autoriteit Consument en Markt (AMC)*	**Definice a požadavky týkající se platnosti souhlasu**	Modernizovaná úmluva č. 108, čl. 5 odst. 2 Doporučení o zdravotních údajích, článek 6 a různá následná doporučení Rozsudek ESLP z roku 2015, *Elberte v. Lotyšsko*, č. 61243/08

*Poznámka: * Rada Evropy, Výbor ministrů (2010): Doporučení CM/Rec(2010)13 Výboru ministrů členským státům o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů v kontextu profilování (doporučení o profilování), 23. listopadu 2010.*

2.1. Osobní údaje

Hlavní body

- Osobními údaji se rozumí takové údaje, které se týkají identifikované nebo identifikovatelné osoby, „subjektu údajů".
- K určení, zda je fyzická osoba identifikovatelná, by správce nebo jiná osoba měli zohlednit veškeré rozumné prostředky, které budou pravděpodobně použity – například výběr vyčleněním – za účelem přímé nebo nepřímé identifikace fyzické osoby.
- Autentizace znamená dokázat, že jistá osoba vlastní určitou identitu a/nebo je oprávněna provádět jisté činnosti.
- Existují zvláštní kategorie údaje, takzvané citlivé osobní údaje, jejichž výčet je uveden v Modernizované úmluvě č. 108 a v právních předpisech EU o ochraně údajů, které vyžadují zvýšenou ochranu, a proto podléhají zvláštnímu právnímu režimu.
- Údaje jsou anonymizovány, pokud se již nevztahují k identifikovanému nebo identifikovatelnému jednotlivci.
- Pseudonymizace je opatření, po jehož provedení nelze osobní údaje přiřadit subjektu údajů bez dalších informací, které jsou uchovávány samostatně. „Klíč", který umožňuje zpětnou identifikaci subjektů údajů, musí být uchováván samostatně a zabezpečeně. Údaje, které prošly procesem pseudonymizace, jsou i nadále osobními údaji. V právu EU neexistuje pojem „pseudonymizované údaje".
- Zásady a pravidla ochrany údajů se nevztahují na anonymizované informace. Vztahují se však na pseudonymizované údaje.

2.1.1. Hlavní aspekty pojmu osobní údaje

Podle práva EU i podle **práva RE** jsou „osobní údaje" definovány jako informace týkající se identifikované nebo identifikovatelné fyzické osoby.[136] Zahrnují informace o osobě, jejíž totožnost je buď zcela zjevná, nebo ji lze zjistit z dalších informací. Při určování, zda je fyzická osoba identifikovatelná, musí správce nebo jiná osoba přihlédnout ke všem prostředkům, o nichž lze rozumně předpokládat, že se použijí pro přímou či nepřímou identifikaci jednotlivce, například výběrem vyčleňováním, který umožňuje zacházet s jednou osobou jinak než s jinou.[137]

Pokud se údaje takovéto osoby zpracovávají, nazývá se tato osoba „subjektem údajů".

Subjekt údajů

Podle práva EU jsou fyzické osoby jedinými subjekty, které požívají ochrany pravidel na ochranu údajů[138], a podle evropského práva v oblasti ochrany údajů jsou chráněni pouze živí lidé.[139] Obecné nařízení o ochraně osobních údajů (GDPR) definuje osobní údaje jako veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

Právo RE, zejména Modernizovaná úmluva č. 108, rovněž odkazuje na ochranu jednotlivců při zpracování jejich osobních údajů. I zde se osobními údaji rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Tato fyzická osoba, jak se o ní pojednává v GDPR a v Modernizované úmluvě č. 108, se v právu na ochranu údajů označuje jako subjekt údajů.

Právnické osoby také požívají určité ochrany. Existuje judikatura ESLP, kde soud vynesl rozsudek ve věci stížností právnických osob, které tvrdily, že bylo porušeno jejich právo na ochranu před využitím jejich údajů podle článku 8 EÚLP. Článek 8 EÚLP zahrnuje jak právo na respektování soukromého a rodinného života, tak i právo na respektování obydlí a korespondence. Soud proto může přezkoumávat případy podle tohoto druhého uvedeného práva, nikoliv podle práva na soukromý život.

136 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 1; Modernizovaná úmluva č. 108, čl. 2 písm. a).

137 Obecné nařízení o ochraně osobních údajů, 26. bod odůvodnění.

138 Tamtéž, s. 1.

139 Tamtéž, 27. bod odůvodnění. Viz také Pracovní skupina zřízená podle článku 29 (2007), *Stanovisko 4/2007 k pojmu osobní údaje*, WP 136, 20.června 2007, s. 22.

Příklad: Věc *Bernh Larsen Holding AS a další v. Norsko*[140] se týkala stížnosti tří norských společností na rozhodnutí daňového orgánu, které jim nařizovalo poskytnout daňovým kontrolorům kopii všech údajů, které jsou uchovávány na počítačovém serveru, který společně používají.

ESLP rozhodl, že tato povinnost ze strany společností, které byly stěžovateli, představovala zásah do jejich práv na respektování „obydlí" a „korespondence" podle článku 8 EÚLP. Soud však dospěl k závěru, že daňové orgány mají účinné a dostatečné záruky proti zneužívání: společnosti, které jsou stěžovateli, mohly být předem informovány; byly přítomné a schopné předložit podání během zásahu na místě a materiál měl být zničen, jakmile byla daňová kontrola provedena. Za těchto okolností bylo dosaženo spravedlivé rovnováhy mezi právem společností-stěžovatelů na respektování „obydlí" a „korespondence" a jejich zájmem na ochraně soukromí osob, které pro ně pracují, na straně jedné a veřejným zájmem na zajištění účinné kontroly pro účely posouzení plnění daňových povinností na straně druhé. Soud proto rozhodl, že nedošlo k porušení článku 8.

Podle Modernizované úmluvy č. 108 se ochrana údajů týká především ochrany fyzických osob, avšak smluvní strany mohou ve svém vnitrostátním právu rozšířit ochranu údajů na právnické osoby, jako jsou podniky a sdružení. Vysvětlující zpráva k Modernizované úmluvě uvádí, že vnitrostátní právo může chránit legitimní zájmy právnických osob tím, že rozšíří oblast působnosti úmluvy na tyto subjekty.[141] **Právo EU v oblasti ochrany údajů** se nevztahuje na zpracování údajů, které se týkají právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby.[142] Směrnice o soukromí a elektronických komunikacích však chrání důvěrný charakter sdělení a oprávněné zájmy právnických osob s ohledem na zvyšující se kapacitu automatického uchovávání a zpracování údajů týkajících se účastníků a uživatelů.[143] Obdobně návrh nařízení o soukromí a elektronických komunikacích rozšiřuje ochranu na právnické osoby.

140 Rozsudek ESLP ze dne 14. března 2013, *Bernh Larsen Holding AS a další v. Norsko*, č. 24117/08. Avšak také viz rozsudek ESLP ze dne 1. července 2008, *Liberty a další v. Spojené království*, č. 58243/00.

141 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 30.

142 Obecné nařízení o ochraně osobních údajů, 14. bod odůvodnění.

143 Směrnice o soukromí a elektronických komunikacích, 7. bod odůvodnění a čl. 1 odst. 2.

Příklad: Ve věci *Volker und Markus Schecke a Hartmut Eifert v. Land Hessen*[144] SDEU s odkazem na zveřejnění osobních údajů příjemců zemědělské podpory rozhodl, že „právnické osoby [se] mohou dovolávat ochrany podle článků 7 a 8 Listiny v souvislosti s takovou identifikací pouze v rozsahu, v němž oficiální název právnické osoby identifikuje jednu nebo více fyzických osob. [...R]espektování práva na soukromý život v souvislosti se zpracováním osobních údajů, přiznaného články 7 a 8 Listiny, [se] vztahuje na veškeré informace o identifikované nebo identifikovatelné fyzické osobě [...]".[145]

SDEU hledal rovnováhu mezi zájmem EU zajistit transparentnost při přidělování podpory na straně jedné a mezi základními právy na soukromí a ochranu údajů, která požívají jednotlivci, kteří podporu čerpali, na straně druhé a rozhodl, že zásah do těchto základních práv byl nepřiměřený. Domníval se, že cíle transparentnosti bylo možné účinně dosáhnout opatřeními, která by méně narušovala práva dotčených jednotlivců. Avšak při přezkumu přiměřenosti zveřejněných informací o právnických osobách, které čerpaly podporu, SDEU dospěl k jinému závěru a rozhodl, že toto zveřejnění neporušuje zásadu přiměřenosti. Uvedl, že „závažnost zásahu do práva na ochranu osobních údajů se totiž projevuje odlišně u právnických osob a u fyzických osob".[146] Právnické osoby podléhaly vyšší míře povinností, pokud jde o zveřejňování informací o těchto osobách. SDEU měl za to, že povinnost vnitrostátních orgánů přezkoumat před dotčeným zveřejněním údajů u každé právnické osoby, která je příjemcem podpory, zda její název identifikuje jakékoliv spřízněné fyzické osoby, by znamenala pro tyto orgány nepřiměřenou administrativní zátěž. Proto právní předpis vyžadující obecné zveřejňování údajů o právnických osobách dosáhl spravedlivé rovnováhy, pokud jde o zohlednění příslušných protichůdných zájmů.

Povaha údajů

Všechny druhy informací mohou být osobními údaji, pokud se vztahují k identifikované nebo identifikovatelné osobě.

144 Rozsudek SDEU (velkého senátu) ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, bod 53.

145 Tamtéž, body 52–53.

146 Tamtéž, bod 87.

Příklad: Hodnocení pracovního výkonu zaměstnance ze strany nadřízeného uložené v osobním spise zaměstnance je osobním údajem o zaměstnanci. Je tomu tak i v případě, že může odrážet zcela nebo částečně osobní názor nadřízeného, například: „zaměstnanec není oddán své práci" – a nikoliv nezpochybnitelné skutečnosti, například: „zaměstnanec nebyl v uplynulých šesti měsících v zaměstnání po dobu pěti týdnů".

Osobními údaji jsou informace týkající se soukromého života dané osoby, což rovněž zahrnuje profesní činnosti, ale také informace o jejím veřejném životě.

Ve věci *Amman*[147] ESLP vyložil pojem „osobní údaje" tak, že není omezen na záležitosti soukromé sféry jednotlivce. Tento význam pojmu „osobní údaje" je též relevantní pro GDPR.

Příklad: Ve věci *Volker und Markus Schecke a Hartmut Eifert v. Land Hessen*[148] SDEU uvedl, že „v tomto ohledu nemá význam skutečnost, že zveřejněné údaje se týkají profesní činnosti [...]. Evropský soud pro lidská práva v tomto ohledu v souvislosti s výkladem článku 8 EÚLP rozhodl, že výraz „soukromý život" nesmí být vykládán restriktivně a „žádný zásadní důvod neumožňuje vyloučit profesní činnost [...] z pojmu soukromý život".

Příklad: Ve spojených věcech *YS v. Minister voor Immigratie, Integratie en Asiel* a *Minister voor Immigratie, Integratie en Asiel v. M. a S.*[149] SDEU uvedl, že právní rozbor obsažený v návrhu rozhodnutí Imigrační a naturalizační služby, jež se zabývalo žádostmi o povolení k pobytu, sám o sobě nepředstavuje osobní údaj, ačkoliv může některé osobní údaje obsahovat.

Judikatura ESLP týkající se článku 8 EÚLP potvrzuje, že může být obtížné zcela oddělit záležitosti soukromého a profesního života.[150]

147 Viz rozsudek ESLP ze dne 16. února 2000, *Amann v. Švýcarsko*, č. 27798/95, bod 65.

148 Rozsudek SDEU (velkého senátu) ze dne 9. listopadu 2010, spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, bod 59.

149 Rozsudek SDEU ze dne 17. července 2014, spojené věci C-141/12 a C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M a S*, bod 39.

150 Viz například rozsudek ESLP (velkého senátu) ze dne 4. května 2000, *Rotaru v. Rumunsko*, č. 28341/95, bod 43; rozsudek ESLP ze dne 16. prosince 1992, *Niemietz v. Německo*, č. 13710/88, bod 29.

Příklad: Ve věci *Bărbulescu v. Rumunsko*[151] byl stěžovatel propuštěn kvůli tomu, že používal internet zaměstnavatele během pracovní doby v rozporu s interními předpisy. Jeho zaměstnavatel sledoval jeho komunikaci a během vnitrostátního řízení byly předloženy záznamy, které obsahovaly zprávy čistě osobní povahy. ESLP konstatoval, že se použije článek 8, a ponechal otevřenou otázku, zda omezující předpisy zaměstnavatele ponechávaly stěžovateli přiměřeně očekávatelné soukromí, ale v každém případě konstatoval, že pokyny zaměstnavatele nemohou omezit soukromý sociální život na pracovišti na nulu. Pokud jde o meritorní stránku, smluvním státům je třeba přiznat široký prostor pro vlastní uvážení, pokud jde o posouzení nutnosti vytvořit právní rámec upravující podmínky, za kterých může zaměstnavatel na pracovišti regulovat komunikaci zaměstnanců nesouvisející s prací – elektronickou nebo jinou. Avšak vnitrostátní orgány musí zajistit, aby zavedení opatření ke sledování korespondence a jiné komunikace zaměstnance ze strany zaměstnavatele, bez ohledu na rozsah a dobu trvání těchto opatření, bylo doprovázeno přiměřenými a dostatečnými zárukami před zneužitím. Stěžejní jsou proporcionalita a procesní záruky před svévolí a ESLP určil řadu faktorů, které byly za daných okolností relevantní. K těmto faktorům patří například rozsah sledování zaměstnanců ze strany zaměstnavatele a míra zásahu do soukromí zaměstnance, důsledky pro zaměstnance a to, zda byly poskytnuty dostatečné záruky. Kromě toho musí vnitrostátní orgány zajistit, aby zaměstnanec, jehož komunikace byla sledována, měl přístup k opravným prostředkům u soudního orgánu, který má soudní příslušnost určit, alespoň v zásadě, jak byla tato nastíněná kritéria dodržována a zda napadená opatření byla zákonná. V této věci ESLP konstatoval, že došlo k porušení článku 8, protože vnitrostátní orgány musí poskytnout dostatečnou ochranu práva stěžovatele na respektování jeho soukromého života a korespondence, a proto nezajistily spravedlivou rovnováhu mezi dotčenými zájmy.

Podle práva EU i **podle práva RE** obsahuje informace údaje o osobě, pokud:

- jednotlivec je touto informací identifikován nebo identifikovatelný nebo
- jednotlivec, ačkoliv nebyl identifikován, může být díky této informaci vybrán vyčleněním tak, že je možné zjistit, kdo je subjektem údajů na základě provedení dalšího výzkumu.

151 Rozsudek ESLP (velkého senátu) ze dne 5. září 2017, *Bărbulescu v. Rumunsko*, č. 61496/08, bod 121.

Oba druhy informací jsou podle evropského práva v oblasti ochrany údajů chráněny stejně. Přímá nebo nepřímá identifikovatelnost jednotlivců vyžaduje průběžné posuzování „s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji".[152] ESLP opakovaně uvedl, že pojem „osobní údaje" podle EÚLP je totožný s pojmem v Úmluvě č. 108, zejména pokud jde o podmínku, že se údaje vztahují k identifikovaným nebo identifikovatelným osobám.[153]

GDPR stanoví, že identifikovatelná je taková fyzická osoba, kterou „lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této osoby".[154] Identifikace tudíž vyžaduje prvky, které popisují osobu tak, že je odlišitelná od všech ostatních osob a rozpoznatelná jako jednotlivec. Jméno osoby je jasným příkladem takového popisného prvku a může danou osobu přímo identifikovat. V některých případech mohou mít jiné vlastnosti podobný účinek jako jméno a umožnit přímou identifikaci osoby. Telefonní číslo, číslo sociálního zabezpečení a číslo poznávací značky vozidla jsou příklady informací, které mohou umožnit identifikaci jednotlivce. Je také možné použít prostředky přiřazování – např. počítačové soubory, cookies a webové nástroje dohledu nad přenosem – za účelem vybrání jednotlivců vyčleněním tím, že se identifikuje jejich chování a jejich návyky. Jak je vysvětleno v jednom stanovisku pracovní skupiny zřízené podle článku 29, „bez jakýchkoli dotazů na jméno a adresu daného jednotlivce je možné tuto osobu zařadit na základě socioekonomických, psychologických, filozofických a dalších kritérií a připisovat jí určitá rozhodnutí, protože kontaktní bod (počítač), který používá, již nezbytně nevyžaduje odhalení její identity v úzkém slova smyslu".[155] Definice osobních údajů podle RE i EU je dostatečně široká, aby zahrnovala všechny možnosti identifikace (a proto všechny stupně identifikovatelnosti).

Příklad: Ve věci *Promusicae v. Telefónica de España*[156] SDEU uvedl, že „není zpochybněno, že sdělení jmen a adres určitých uživatelů [určité internetové platformy pro sdílení souborů], o které žádá sdružení Promusicae, s sebou

152 Obecné nařízení o ochraně osobních údajů, 26. bod odůvodnění.

153 Viz rozsudek ESLP (velkého senátu) ze dne 16. února 2000, *Amann v. Švýcarsko*, č. 27798/95, bod 65.

154 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 1.

155 Pracovní skupina zřízená podle článku 29, Stanovisko 4/2007 k pojmu osobní údaje, WP 136, 20. června 2007, s. 15.

156 Rozsudek SDEU (velkého senátu) ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, bod 45.

nese poskytnutí osobních údajů, tzn. informací o identifikovaných nebo identifikovatelných fyzických osobách v souladu s definicí uvedenou v čl. 2 písm. a) směrnice 95/46/ES [nyní čl. 4 bod 1 GDPR]. Toto sdělení informací, které jsou podle sdružení Promusicae uchovávány společností Telefónica – což posledně uvedená nezpochybňuje – představuje zpracování osobních údajů."[157]

Příklad: Věc *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] se týkala toho, že poskytovatel internetových služeb Scarlet odmítl zavést systém filtrování elektronických komunikací, které používají software pro sdílení údajů, za účelem zamezení výměně souborů porušujících autorská práva ze strany společnosti SABAM, což je správcovská společnost, která zastupuje autory, skladatele a vydavatele. SDEU rozhodl, že IP adresy uživatelů „jsou vzhledem k tomu, že umožňují přesně určit totožnost uvedených uživatelů, chráněnými osobními údaji".

Jelikož řada jmen není jedinečných, zjištění totožnosti osoby může vyžadovat další prostředky přiřazování, aby bylo zajištěno, že nedošlo k omylu. Někdy může být nutné kombinovat přímé a nepřímé prostředky přiřazování za účelem identifikace osoby, k níž se informace vztahují. Často se používá datum a místo narození. Kromě toho byla v některých zemích zavedena osobní čísla, která umožňují lépe rozlišovat občany. Předané daňové údaje[159], údaje týkající se žadatele o povolení k pobytu obsažené ve správním dokumentu[160] a dokumenty týkající se bankovních a fiduciárních vztahů[161] mohou být osobními údaji. V technologickém věku se stále častěji používají k identifikaci osob biometrické údaje, jako jsou otisky prstů, digitální fotografie nebo skeny oční duhovky, lokační údaje a on-line prostředky přiřazování.

Aby se však uplatnilo evropské právo v oblasti ochrany údajů, není nutná vlastní identifikace subjektu údajů; stačí, že je dotčená osoba identifikovatelná. Dotčená osoba je identifikovatelná, pokud je k dispozici dostatečný počet prvků, jimiž může

157 Někdejší směrnice 95/46/ES, čl. 2 písm. b), nyní obecné nařízení o ochraně osobních údajů, čl. 4 bod 2.

158 Rozsudek SDEU ze dne 24. listopadu 2011, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, bod 51.

159 Rozsudek SDEU ze dne 1. října 2015, C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*.

160 Rozsudek SDEU ze dne 17. července 2014, *YS v. Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M. a S.*

161 Rozsudek ESLP ze dne 7. července 2015, *M.N. a další v. San Marino*, č. 28005/12.

být daná osoba přímo nebo nepřímo identifikována.[162] Podle 26. bodu odůvodnění GDPR je referenčním kritériem to, zda je pravděpodobné, že budou k dispozici přiměřené prostředky k identifikaci a zda předpokládaní uživatelé této informace budou těmito prostředky disponovat. To zahrnuje informace v držení příjemců, kteří jsou třetími stranami (viz oddíl 2.3.2).

Příklad: Místní orgán se rozhodne, že bude shromažďovat údaje o vozidlech překračujících rychlost v místních ulicích. Fotografuje vozidla, automaticky zaznamenává čas a místo, aby mohl tyto údaje předat příslušnému orgánu, který pak může dát pokutu těm, kteří překročili povolenou rychlost. Subjekt údajů podá stížnost s odůvodněním, že daný místní orgán nemá žádný právní základ podle práva v oblasti ochrany údajů pro takovéto shromažďování údajů. Místní orgán namítne, že neshromažďuje osobní údaje. Státní poznávací značky jsou anonymní, říká. Místní orgán nemá ze zákona oprávnění získat přístup do obecného rejstříku vozidel, aby zjistil totožnost majitele nebo řidiče vozidla.

Toto odůvodnění není v souladu s 26. bodem odůvodnění GDPR. Vzhledem k tomu, že účelem shromažďování údajů je zjevně identifikovat a pokutovat řidiče, kteří překročí rychlost, dá se předpokládat, že dojde k pokusu o identifikaci. Ačkoliv místní orgány nemají k dispozici prostředky, jak provést přímou identifikaci, předají údaje příslušnému orgánu, policii, která takovéto prostředky má. 26. bod odůvodnění výslovně uvádí scénář, kdy se dá očekávat, že se o identifikaci jednotlivce mohou pokusit další příjemci údajů jiní než bezprostřední uživatel údajů. Vzhledem k ustanovením 26. bodu odůvodnění se jednání místního orgánu považuje za shromažďování údajů o identifikovatelných osobách, a proto se vyžaduje právní základ podle práva v oblasti ochrany údajů.

„Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji.“[163]

162 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 1.

163 Tamtéž, 26. bod odůvodnění.

Příklad: Ve věci *Breyer v. Bundesrepublik Deutschland*[164] SDEU rozebíral pojem nepřímá identifikovatelnost subjektů údajů. Případ se týkal dynamických IP adres, které se mění s každým novým připojením k internetu. Webové stránky spravované spolkovými německými orgány registrovaly a ukládaly dynamické IP adresy s cílem zabránit kybernetickým útokům a případně s cílem zahájit trestní řízení. Pouze poskytovatel internetových služeb, jehož služeb využíval pan Breyer, měl doplňující údaje, které byly zapotřebí k identifikaci uživatele.

SDEU zvažoval, zda dynamická IP adresa, kterou registruje poskytovatel on-line mediálních služeb, když daná osoba navštíví webové stránky, a kterou poskytovatel zpřístupnil veřejnosti, představuje osobní údaje pouze tehdy, pokud třetí strana – v tomto případě poskytovatel internetových služeb – má dodatečné údaje, které jsou nezbytné k identifikaci dané osoby.[165] Rozhodl, že k tomu, aby informace představovala osobní údaje, „není požadováno, aby se všechny informace umožňující identifikovat subjekt údajů musely nacházet v rukách jediné osoby". Uživatelé dynamické IP adresy registrovaní poskytovatelem internetových služeb mohou být identifikováni v jistých situacích, například v rámci trestního řízení v případě kybernetických útoků, za pomoci jiných osob.[166] Podle SDEU, pokud poskytovatel „má k dispozici právní prostředky, které mu umožňují identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu", jedná se o prostředek, který může být rozumně použit pro identifikaci subjektu údajů". Proto se tyto údaje považují za osobní údaje.

Právo RE chápe identifikovatelnost podobně. Vysvětlující zpráva k Modernizované úmluvě č. 108 obsahuje podobný popis: pojem „identifikovatelný" se nevztahuje pouze k civilní nebo právní identitě jednotlivce jako takové, ale také k tomu, co může umožnit „individualizaci" jisté osoby nebo její výběr vyčleněním ze skupiny jiných, a tudíž může vést k odlišnému zacházení. Tuto „individualizaci" je možné provést například odkazem na tuto osobu konkrétně nebo na zařízení nebo kombinaci zařízení (počítač, mobilní telefon, fotoaparát, herní zařízení atd.) spojených

164 Rozsudek SDEU ze dne 19. října 2016, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, bod 47–48.

165 Někdejší směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, čl. 2 písm. a).

166 Rozsudek SDEU ze dne 24. listopadu 2011, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, body 47–48.

s identifikačním číslem, přezdívkou, biometrickými nebo genetickými údaji, lokačními údaji, IP adresou nebo jiným identifikátorem.[167] Jednotlivec se nepovažuje za „identifikovatelného", pokud je k jeho identifikaci nutné vynaložit nepřiměřené množství času, úsilí nebo zdrojů. Tak je tomu například v případě, kdy by identifikace subjektu údajů vyžadovala nadměrně složité, dlouhé a nákladné operace. Nepřiměřený čas, úsilí nebo zdroje musí být posuzovány v každém jednotlivém případě a je třeba při tom zohledňovat faktory, jako je účel zpracování, náklady a přínosy identifikace, druh správce a použitou technologii.[168]

Pokud jde o formu, v níž jsou osobní údaje ukládány a uchovávány, je důležité připomenout, že tato okolnost není relevantní, pokud jde o uplatnění práva v oblasti ochrany údajů. Psaná nebo mluvená sdělení mohou obsahovat osobní údaje stejně jako obrazové záznamy[169], včetně záznamu z uzavřeného televizního okruhu (CCTV)[170] nebo zvukového záznamu[171]. Rovněž mohou být osobními údaji informace zaznamenané elektronicky a informace na papíře. Dokonce i vzorky buněk lidské tkáně – které zaznamenávají DNA dané osoby – mohou být zdrojem, z něhož lze získat biometrické údaje[172], pokud se tyto údaje vztahují ke zděděným nebo získaným genetickým charakteristikám daného jednotlivce, poskytují jedinečnou informaci o jejich zdraví nebo fyziologii a jsou výsledkem analýzy biologického vzorku dané osoby.[173]

Anonymizace

Podle zásady omezení uložení obsažené v GDPR i v Modernizované úmluvě č. 108 (podrobněji o této zásadě pojednává kapitola 3) musí být údaje uloženy „ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely,

167 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 18.

168 Tamtéž, bod 17.

169 Rozsudek ESLP ze dne 24. června 2004, *Von Hannover v. Německo*, č. 59320/00; rozsudek ESLP ze dne 11. ledna 2005, *Sciacca v. Itálie*, č. 50774/99; rozsudek SDEU ze dne 11. prosince 2014, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*.

170 Rozsudek ESLP ze dne 28. ledna 2003, *Peck v. Spojené království*, č. 44647/98; rozsudek ESLP ze dne 5. října 2010, *Köpke v. Německo* (dec.), č. 420/07; EIOÚ (2010), *The EDPS video-surveillance guidelines [Pokyny EIOÚ ke sledování videotechnikou]*, 17. března 2010.

171 Rozsudek ESLP ze dne 25. září 2001, *P. G. a J. H. v. Spojené království*, č. 44787/98, body 59–60; rozsudek ESLP ze dne 20. prosince 2005, *Wisse v. Francie*, č. 71611/01 (francouzské jazykové znění).

172 Viz Pracovní skupina zřízená podle článku 29 (2007), Stanovisko 4/2007 k pojmu osobní údaje, WP 136, 20. června 2007, s. 9; Rada Evropy, Doporučení č. Rec(2006)4 Výboru ministrů členským států týkající se výzkumu biologických materiálů lidského původu, 15. března 2006.

173 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 13.

pro které jsou zpracovávány“.[174] Údaje je tedy nutné smazat nebo anonymizovat, pokud je správce chce uložit poté, co již nejsou nutné a neslouží svému původnímu účelu.

Proces anonymizace údajů znamená, že ze souboru osobních údajů jsou odstraněny všechny identifikující prvky, aby již nebylo možné identifikovat subjekt údajů.[175] Ve svém stanovisku 05/2014 pracovní skupina zřízená podle článku 29 analyzuje účinnost a meze jednotlivých technik anonymizace.[176] Uznává potenciální hodnotu těchto technik, ale zdůrazňuje, že některé techniky nemusí nutně ve všech případech fungovat. O optimálním řešení v dané situaci a vhodném procesu anonymizace je třeba rozhodnout v každém jednotlivém případě. Bez ohledu na použitou techniku je třeba nezvratně zabránit identifikaci. To znamená, že aby byly údaje anonymizovány, nesmí být v těchto informacích ponechán žádný prvek, který by při vynaložení přiměřeného úsilí posloužil k opětovné identifikaci dotčené osoby (osob).[177] Riziko opětovné identifikace je možné posoudit s ohledem na „čas, úsilí nebo zdroje nutné vzhledem k povaze údajů, kontext jejich užívání, dostupnost technologií pro opětovnou identifikaci a související náklady“.[178]

Jakmile byly údaje úspěšně anonymizovány, již se nejedná o osobní údaje a nevztahují se na ně právní předpisy o ochraně údajů.

GDPR stanoví, že osoba řídící zpracování osobních údajů nesmí mít povinnost uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů výlučně kvůli dosažení souladu s tímto nařízením. Z tohoto pravidla však platí významná výjimka: kdykoliv subjekt údajů za účelem výkonu práva na přístup, opravu nebo výmaz, omezení zpracování a přenositelnost údajů poskytne dodatečné informace správci, které umožní jeho identifikaci, pak tyto údaje, které byly dříve anonymizovány, se znovu stanou osobními údaji.[179]

174 Tamtéž, čl. 5 odst. 1 písm. e); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. e).

175 Obecné nařízení o ochraně osobních údajů, 26. bod odůvodnění.

176 Pracovní skupina zřízená podle článku 29 (2014), *Stanovisko č. 5/2014 k technikám anonymizace*, WP 216, 10. dubna 2014.

177 Obecné nařízení o ochraně osobních údajů, 26. bod odůvodnění.

178 Rada Evropy, Výbor podle Úmluvy č. 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu]*, 23. ledna 2017, bod 6.2.

179 Obecné nařízení o ochraně osobních údajů, článek 11.

Pseudonymizace

Osobní informace obsahují prostředky přiřazování, jako je jméno, datum narození, pohlaví, adresa nebo jiné prvky, které by mohly vést k identifikaci. Proces pseudonymizace osobních údajů znamená, že se tyto prostředky přiřazování nahradí pseudonymem.

Právo EU definuje „pseudonymizaci" jako „zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě".[180] Narozdíl od anonymizovaných údajů jsou ty pseudonymizované stále osobními údaji, a proto se řídí právními předpisy v oblasti ochrany údajů. Ačkoliv pseudonymizace může omezit bezpečnostní rizika hrozící subjektům údajů, nenachází se mimo oblast působnosti GDPR.

GDPR uznává různá použití pseudonymizace jakožto vhodného technického opatření na posílení ochrany údajů a pseudonymizace je výslovně zmíněna, pokud jde o návrh a bezpečnost zpracování údajů.[181] Jedná se také o vhodnou záruku, která by mohla být použita ke zpracování osobních údajů pro jiné účely, než pro které byly původně shromážděny.[182]

V právních definicích Modernizované úmluvy **RE** č. 108 není pseudonymizace výslovně uvedena. Avšak ve Vysvětlující zprávě k Modernizované úmluvě č. 108 se jasně uvádí, že „používání pseudonymu nebo jiného digitálního identifikátoru / digitální identity nemá za následek anonymizaci údajů, protože subjekt údajů lze stále identifikovat nebo individualizovat".[183] Jednou možností, jak pseudonymizovat údaje, je využít šifrování údajů. Jakmile jsou údaje pseudonymizovány, odkaz na identitu existuje ve formě pseudonymu a šifrovacího klíče. Bez tohoto klíče je obtížné určit pseudonymizované údaje. Osoby, které jsou oprávněné používat dešifrovací klíč, však snadno mohou provést zpětnou identifikaci. Je třeba především zabránit tomu, aby šifrovací klíče používaly neoprávněné osoby. Proto „[j]e nutné […] považovat

180 Tamtéž, čl. 4 bod 5.

181 Tamtéž, čl. 25 odst. 1.

182 Tamtéž, čl. 6 odst. 4.

183 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 18.

pseudonymizované údaje za osobní údaje [...]", na které se vztahuje Modernizovaná úmluva č. 108.[184]

Autentizace

Jedná se o proces, jímž je osoba schopna prokázat, že vlastní určitou identitu a/nebo je oprávněna provádět některé úkony, například vstoupit do zabezpečeného prostoru nebo vybrat peníze z bankovního účtu. Autentizace lze dosáhnout porovnáním biometrických údajů, jako je fotografie v cestovním pasu, s údaji osoby, která se dostaví například na kontrolu imigrace;[185] nebo tím, že je požádána o informace, které by měly být známy pouze osobě s určitou identitou nebo oprávněním, jako je osobní identifikační číslo (PIN) nebo heslo; nebo tím, že se požaduje předložení určitého tokenu, který by měl být výlučně ve vlastnictví osoby s určitou identitou nebo oprávněním, např. zvláštní čipová karta nebo klíč k bankovní úložné schránce. Kromě hesel nebo čipových karet jsou vhodným nástrojem, který je schopen provést zejména identifikaci a autentizaci osoby v elektronické komunikaci, elektronické podpisy – někdy spolu s číslem PIN.

2.1.2. Zvláštní kategorie osobních údajů

Podle práva EU i podle **práva RE** existují zvláštní kategorie osobních údajů, které ze své podstaty při zpracovávání představují riziko pro subjekty údajů a které vyžadují posílenou ochranu. Tyto údaje podléhají zásadě zákazu a existuje omezený počet podmínek, za nichž je jejich zpracování zákonné.

V rámci Modernizované úmluvy č. 108 (článek 6) a GDPR (článek 9) se za citlivé osobní údaje považují tyto kategorie:

- osobní údaje, které vypovídají o rasovém či etnickém původu,
- osobní údaje, které vypovídají o politických názorech, náboženském nebo jiném přesvědčení, včetně filozofického,
- osobní údaje, které vypovídají o členství v odborech,
- genetické údaje a biometrické údaje za účelem identifikace dané osoby,

184 Tamtéž.

185 Tamtéž, body 56–57.

- údaje o zdravotním stavu, o sexuálním životě nebo sexuální orientaci.

Příklad: Věc *Bodil Lindqvist*[186] se týkala odkazu na různé osoby na jisté webové stránce pomocí jména nebo jinými prostředky, jako je jejich telefonní číslo nebo informace o jejich koníčcích. SDEU uvedl, že „údaj o tom, že se určitá osoba zranila na noze a čerpá částečné volno z důvodu nemoci, je osobním údajem týkajícím se zdraví".[187]

Osobní údaje týkající se odsouzení za trestný čin a trestných činů

Modernizovaná úmluva č. 108 se vztahuje i na osobní údaje týkající se trestných činů, trestněprávních řízení a odsouzení za trestný čin a souvisejících bezpečnostních opatření na seznamu zvláštních kategorií osobních údajů.[188] V rámci GDPR nejsou osobní údaje týkající se odsouzení za trestný čin a trestných činů nebo souvisejících bezpečnostních opatření uvedeny jako takové v seznamu zvláštních kategorií údajů, ale pojednává o nich samostatný článek. Článek 10 GDPR stanoví, že zpracování těchto údajů může být prováděno pouze „pod dozorem orgánu veřejné moci, nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů". Na druhou stranu souhrnné rejstříky trestů mohou být vedeny pouze pod dozorem konkrétních orgánů veřejné moci.[189] V EU se zpracování osobních údajů v souvislosti s prosazováním práva řídí zvláštním právním nástrojem, směrnicí (EU) 2016/680.[190] Tato směrnice stanoví konkrétní pravidla pro ochranu údajů, která jsou pro příslušné orgány závazná, pokud zpracovávají osobní údaje zvlášť za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů (viz oddíl 8.2.1).

186 Rozsudek SDEU ze dne 6. listopadu 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*, bod 51.

187 Někdejší směrnice 95/46/ES, čl. 8 odst. 1, nyní obecné nařízení o ochraně osobních údajů, čl. 9 odst. 1.

188 Modernizovaná úmluva č. 108, čl. 6 odst. 1.

189 Obecné nařízení o ochraně osobních údajů, článek 10.

190 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, Úř. věst. 2016 L 119.

2.2. Zpracování údajů

Hlavní body

- „Zpracování údajů" se týká každé operace provedené s osobními údaji.
- Pojem „zpracování" zahrnuje automatizované i neautomatizované zpracování.
- Podle práva EU znamená „zpracování" také manuální zpracování ve strukturované evidenci.
- Podle práva RE lze význam „zpracování" rozšířit v rámci vnitrostátního práva tak, aby zahrnovalo manuální zpracování.

2.2.1. Pojem zpracování údajů

Pojem zpracování osobních údajů je komplexní **jak podle práva EU, tak podle práva RE**: „‚zpracováním' [se rozumí] jakákoliv operace [...], jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení"[191] osobních údajů. Modernizovaná úmluva č. 108 přidává do definice uchovávání osobních údajů.[192]

Příklad: Ve věci *František Ryneš*[193] zaznamenal pan Ryneš snímek dvou osob, které rozbily okna jeho domova, prostřednictvím domácího systému sledování CCTV, který nainstaloval za účelem ochrany svého majetku. SDEU rozhodl, že monitorování prostřednictvím obrazového záznamu, včetně zaznamenávání a ukládání osobních údajů představuje automatizované zpracování údajů, které spadá do působnosti práva EU v oblasti ochrany údajů.

Příklad: Ve věci *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*[194] požádal pan Manni o odstranění svých osobních údajů z rejstříku společnosti specializující se na rating, které ho spojovaly

191 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 2. Viz také Modernizovanou úmluvu č. 108, čl. 2 písm. b).

192 Modernizovaná úmluva č. 108, čl. 2 písm. b).

193 Rozsudek SDEU ze dne 11. prosince 2014, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, bod 25.

194 Rozsudek SDEU ze dne 9. března 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, bod 35.

s likvidací realitní společnosti, a měly tudíž negativní dopad na jeho dobrou pověst. SDEU rozhodl, že „zápisem a uchováním uvedených informací v rejstříku a případně jejich sdělením na žádost třetím osobám provádí orgán pověřený vedením tohoto rejstříku ‚zpracování osobních údajů', za které je ‚odpovědný'".

Příklad: Zaměstnavatelé shromažďují a zpracovávají údaje o svých zaměstnancích, včetně informací týkajících se jejich platů. Jejich pracovní smlouva stanoví právní základ pro legitimní zpracovávání.

Zaměstnavatelé následně budou muset předat údaje o platech zaměstnanců daňovým orgánům. Předání údajů bude rovněž představovat „zpracování" ve smyslu tohoto pojmu uvedeného v Modernizované úmluvě č. 108 a v GDPR. Právním základem pro toto zveřejnění však nejsou pracovní smlouvy. Musí existovat další právní základ pro operace zpracování, na jejichž základě zaměstnavatel předá údaje o platech daňovým orgánům. Tento právní základ se obvykle nachází v ustanoveních vnitrostátní právní úpravy v oblasti daní. Bez těchto ustanovení – a v případě, že neexistuje jiný legitimní důvod pro zpracování – by toto předání osobních údajů představovalo protiprávní zpracování.

2.2.2. Automatizované zpracování údajů

Ochrana údajů podle Modernizované úmluvy č. 108 a GDPR se v plné míře uplatní na automatizované zpracování údajů.

Podle **práva EU** se automatizované zpracování údajů vztahuje na operace „zcela nebo částečně automatizované[ho] zpracování osobních údajů".[195] Modernizovaná úmluva č. 108 obsahuje podobnou definici.[196] To prakticky znamená, že na veškeré zpracování osobních údajů automatickými prostředky pomocí například osobních počítače, mobilního zařízení nebo routeru se vztahují pravidla ochrany údajů jak EU, tak RE.

195 Obecné nařízení o ochraně osobních údajů, čl. 2 odst. 1 a čl. 4 bod 2.

196 Modernizovaná úmluva č. 108, čl. 2 písm. b) a c); Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 21.

Příklad: Věc *Bodil Lindqvist*[197] se týkala odkazu na různé osoby na jisté webové stránce pomocí jména nebo jinými prostředky, jako je jejich telefonní číslo nebo informace o jejich koníčcích. SDEU rozhodl, že „úkon, který spočívá v tom, že se na webové stránce odkáže na různé osoby, které jsou identifikovány buď svým jménem, nebo jinými prostředky, například telefonním číslem nebo údaji o pracovních poměrech a zálibách, je ‚zcela nebo částečně automatizovaným zpracováním osobních údajů'" ve smyslu čl. 3 odst. 1 směrnice 95/46/ES.[198]

Příklad: Ve věci *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[199] požádal pan González o odstranění nebo změnu spojitosti mezi jeho jménem ve vyhledávači Google a dvěma novinovými stranami oznamujícími dražbu nemovitostí zabavených v důsledku dluhů na sociálním zabezpečení. SDEU konstatoval, že „automatickým, neustálým a systematickým prohlížením internetu za účelem vyhledávání tam zveřejněných informací provozovatel vyhledávače ‚shromažďuje' takové údaje, které ‚vyhledává', ‚zaznamenává' a následně v rámci svých programů indexování ‚uspořádává', ‚uchovává' na svých serverech a případně ‚sděluje' a ‚zpřístupňuje' svým uživatelům ve formě seznamů výsledků jejich vyhledávání".[200] SDEU dospěl k závěru, že tyto úkony představují „zpracování", „aniž je důležité, zda vyhledávač používá tytéž úkony rovněž na další druhy informací a nerozlišuje mezi nimi a osobními údaji".

2.2.3. Neautomatizované zpracování údajů

I manuální zpracování údajů vyžaduje ochranu údajů.

Ochrana údajů **podle práva EU** není v žádném případě omezena na automatizované zpracování údajů. Proto se podle práva EU ochrana údajů vztahuje na zpracování osobních údajů v manuální evidenci, tj. ve zvláštním způsobem strukturované složce papírů.[201] Strukturovaná evidence je taková, která třídí soubory osobních údajů do kategorií a zpřístupňuje je podle určitých kritérií. Například pokud zaměstnavatel

197 Rozsudek SDEU ze dne 6. listopadu 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*, bod 27.

198 Obecné nařízení o ochraně osobních údajů, čl. 2 odst. 1.

199 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

200 Tamtéž, bod 28.

201 Obecné nařízení o ochraně osobních údajů, čl. 2 odst. 1.

vede papírovou složku s názvem „dovolená zaměstnanců“, která obsahuje veškeré podrobnosti o dovolených, které si zaměstnanci vybrali v uplynulém roce, a je setříděna podle abecedy, představuje tato složka manuální evidenci, která podléhá pravidlům EU v oblasti ochrany údajů. Důvodem pro toto rozšíření ochrany údajů je, že:

- papírové složky mohou být strukturovány tak, aby urychlovaly a usnadňovaly dohledávání informací,

- ukládání osobních údajů do strukturovaných papírových složek usnadňuje obcházení omezení stanovených zákonem pro automatizované zpracování údajů.[202]

Podle **práva RE** uznává definice automatizovaného zpracovávání, že mezi operacemi automatizovaného zpracovávání mohou být nutné některé fáze manuálního využívání osobních údajů.[203] Článek 2 písm. c) Modernizované úmluvy č. 108 stanoví, že „[p]okud se nevyužívá automatizované zpracování, znamená „zpracování údajů“ jakoukoliv operaci nebo soubor operací provedených s osobními údaji v rámci strukturovaného souboru takových údajů, které jsou přístupné nebo je možné je vyhledat podle určitých kritérií“.

2.3. Uživatelé osobních údajů

Hlavní body

- Osoba, která určuje prostředky a účely zpracování osobních údajů jiných osob, je podle práva v oblasti ochrany údajů „správcem“. Pokud toto rozhodnutí činí několik osob současně, může se jednat o „společné správce“.

- „Zpracovatel“ je fyzická nebo právnická osoba, která zpracovává osobní údaje jménem správce.

- Zpracovatel se stává správcem, pokud určuje prostředky a účely samotného zpracování údajů.

- Každá osoba, jíž jsou sděleny osobní údaje, je „příjemcem“.

202 Obecné nařízení o ochraně osobních údajů, 15. bod odůvodnění.

203 Modernizovaná úmluva č. 108, čl. 2 písm. b) a c).

- „Třetí strana“ je fyzická nebo právnická osoba, která není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.
- Souhlas jako právní základ pro zpracování osobních údajů musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle formou zjevného potvrzení svolení ke zpracování.
- Zpracování zvláštních kategorií údajů na základě souhlasu vyžaduje výslovný souhlas.

2.3.1. Správci a zpracovatelé

Nejdůležitějším důsledkem nabytí funkce správce nebo zpracovatele je právní odpovědnost za dodržování příslušných povinností podle práva v oblasti ochrany údajů. V soukromém sektoru jde obvykle o fyzickou nebo právnickou osobu, ve veřejném sektoru jde obvykle o orgán. Existuje významný rozdíl mezi správcem údajů a zpracovatelem údajů: správce je fyzická nebo právnická osoba, která určuje účely a prostředky zpracování, zatímco zpracovatel je fyzická nebo právnická osoba, která zpracovává údaje jménem správce a důsledně plní pokyny. V zásadě právě správce údajů musí uplatňovat dohled nad zpracováním a nese za ně odpovědnost, včetně té právní. Po reformě pravidel v oblasti ochrany údajů však zpracovatelé nyní mají povinnosti jednat v souladu s řadou požadavků, které se týkají správců. Například podle GDPR musí zpracovatelé vést záznamy o všech kategoriích činností zpracování, aby prokázali, že jednají v souladu se svými povinnostmi podle tohoto nařízení.[204] Zpracovatelé také musí zavést technická a organizační opatření pro zajištění bezpečnosti zpracování[205], za jistých okolností jmenovat pověřence pro ochranu osobních údajů[206] a oznamovat správci porušení zabezpečení[207].

To, zda má daná osoba pravomoc rozhodnout o účelu a prostředcích zpracování a určit je, bude záležet na situaci nebo skutkových okolnostech dané věci. Podle definice správce uvedené v GDPR mohou být správcem fyzické osoby, právnické osoby nebo jakékoliv jiné subjekty. Avšak pracovní skupina zřízená podle článku 29 zdůraznila, že aby jednotlivci měli k dispozici stabilnější subjekt pro účely výkonu svých práv, „je třeba dát přednost tomu, zvážit jako správce společnost nebo orgán jako takový, nikoliv konkrétní osobu působící v rámci této společnosti nebo

204 Obecné nařízení o ochraně osobních údajů, čl. 30 odst. 2.

205 Tamtéž, článek 32.

206 Tamtéž, článek 37.

207 Tamtéž, čl. 33 odst. 2.

orgánu".[208] Například společnost prodávající zdravotnické potřeby zdravotnickým pracovníkům je správcem, který sestavuje a spravuje distribuční seznam všech zdravotnických pracovníků v určité oblasti, a nikoliv manažer prodeje, který tento seznam reálně používá a spravuje.

Příklad: Když marketingové oddělení společnosti Sunshine plánuje zpracovávat údaje za účelem průzkumu trhu, nebudou správcem tohoto zpracování zaměstnanci marketingového oddělení, ale společnost Sunshine. Marketingové oddělení nemůže být správcem, protože nemá samostatnou identitu.

Fyzické osoby mohou být správci podle práva EU i RE. Avšak při zpracování údajů o jiných osobách v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti nespadají soukromé osoby do působnosti pravidel stanovených v GDPR ani v Modernizované úmluvě č. 108 a nepovažují se za správce.[209] Jednotlivec vedoucí svou korespondenci, osobní deník popisující incidenty s přáteli a kolegy a zdravotní záznamy rodinných příslušníků mohou být vyňaty z působnosti pravidel v oblasti ochrany údajů, protože tyto činnosti by mohly být v rámci činností čistě osobní povahy nebo činností prováděných výhradně v domácnosti. GDPR dále upřesňuje, že činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti mohou také zahrnovat využívání sociálních sítí a internetu v souvislosti s těmito činnostmi.[210] Naopak se pravidla zpracování údajů v plné míře vztahují na správce a zpracovatele, kteří poskytují prostředky ke zpracování osobních údajů pro činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti (například platformy sociálních sítí).[211]

Přístup občanů k internetu a možnost využívat platformy elektronického obchodování, sociální sítě a stránky pro vytváření blogů za účelem sdílení osobních informací o sobě a o jiných jednotlivcích stále více ztěžuje oddělení osobního zpracování od neosobního.[212] To, zda jsou činnosti čistě osobní povahy nebo prováděné

208 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010.

209 Obecné nařízení o ochraně osobních údajů, 18. bod odůvodnění a čl. 2 odst. 2 písm. c); Modernizovaná úmluva č. 108, čl. 3 odst. 2.

210 Obecné nařízení o ochraně osobních údajů, 18. bod odůvodnění.

211 Tamtéž, 18. bod odůvodnění; Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 29.

212 Viz prohlášení pracovní skupiny zřízené podle článku 29 k diskusím o balíčku právních předpisů reformujících ochranu údajů (2013), *Příloha 2:* Návrhy a pozměňovací návrhy týkající se výjimky pro činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, 27. února 2013.

výhradně v domácnosti, záleží na okolnostech.[213] Na činnosti, které mají profesní nebo obchodní aspekty, se nemůže vztahovat výjimka pro domácnosti.[214] Pokud tudíž rozsah a četnost zpracování údajů svědčí o profesionální činnosti nebo činnosti na plný úvazek, měla by být soukromá osoba považována za správce. Kromě profesní nebo obchodní povahy činnosti zpracování, je třeba též zohlednit další aspekt, a sice zda jsou osobní údaje zpřístupněny velkému počtu osob, které se zjevně nachází mimo soukromou sféru daného jednotlivce. Judikatura týkající se směrnice o ochraně údajů dospěla k závěru, že právo v oblasti ochrany údajů se použije tehdy, pokud soukromá osoba v průběhu používání internetu zveřejní údaje o jiných osobách na veřejné webové stránce. SDEU dosud nerozhodl o podobných skutkových okolnostech podle GDPR, které stanoví podrobnější pokyny k tématům, která je možné považovat za témata nacházející se mimo oblast působnosti právních předpisů v oblasti ochrany údajů podle „výjimky pro domácnosti", například používání sociálních médií pro osobní účely.

Příklad: Věc *Bodil Lindqvist*[215] se týkala odkazu na různé osoby na jistě webové stránce pomocí jména nebo jinými prostředky, jako je jejich telefonní číslo nebo informace o jejich koníčcích. SDEU potvrdil, že „úkon, který spočívá v tom, že se na webové stránce odkáže na různé osoby, které jsou identifikovány buď svým jménem, nebo jinými prostředky, [...] je ‚zcela nebo částečně automatizovaným zpracováním osobních údajů'" ve smyslu čl. 3 odst. 1 směrnice o ochraně údajů.[216]

Toto zpracování osobních údajů nepatří výlučně k činnostem čistě osobní povahy nebo prováděným výlučně v domácnosti, jež jsou mimo oblast působnosti právních předpisů EU v oblasti ochrany údajů, protože tato výjimka „[...] musí být vykládána tak, že se týká pouze činností v rámci soukromého nebo rodinného života jednotlivců, což zjevně neplatí pro zpracování osobních údajů, jež spočívá v jejich zveřejnění na internetu tak, že se zpřístupní neomezenému počtu osob".[217]

213 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 28.

214 Viz obecné nařízení o ochraně osobních údajů, 18. bod odůvodnění a Vysvětlující zprávu k Modernizované úmluvě č. 108, bod 27.

215 Rozsudek SDEU ze dne 6. listopadu 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*.

216 Tamtéž, bod 27; někdejší směrnice 95/46/ES, čl. 3 odst. 1, nyní obecné nařízení o ochraně osobních údajů, čl. 2 odst. 1.

217 Rozsudek SDEU ze dne 6. listopadu 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*, bod 47.

Podle SDEU může vizuální záznam bezpečnostní kamery nainstalované k soukromým účelům za určitých okolností spadat do působnosti právních předpisů EU na ochranu údajů.

Příklad: Ve věci *František Ryneš*[218] zaznamenal pan Ryneš snímek dvou osob, které rozbily okna jeho domova, prostřednictvím domácího systému sledování CCTV, který nainstaloval za účelem ochrany svého majetku. Záznam byl následně předán policii a vycházelo z něho trestní řízení.

SDEU uvedl, že „[j]estliže takový kamerový systém, jako je systém [...] zabírá – třebaže částečně – veřejné prostranství, a je tudíž zaměřen mimo soukromou sféru osoby, která jeho prostřednictvím zpracovává údaje, nelze jeho provozování považovat za výlučně ‚osobní či domácí' činnost [...]".[219]

Správce

Podle práva EU je správce definován jako osoba, která „s[ama] nebo společně s jinými určuje účely a prostředky zpracování osobních údajů".[220] Správce svým rozhodnutím určí, proč a jak se budou údaje zpracovávat.

Podle práva RE je v Modernizované úmluvě č. 108 stanoveno, že „správce" je „fyzick[á] nebo právnick[á] osob[a], orgán veřejné moci, poskytovatel služeb, agentur[a] nebo jakýkoliv jiný subjekt, který má sám nebo společně s jinými subjekty pravomoc rozhodovat o zpracování osobních údajů".[221] Tyto rozhodovací pravomoci se týkají účelu a postupů zpracování, jakož i kategorií údajů, které mají být zpracovány, a přístupu k údajům.[222] Zda tyto pravomoci vyplývají z právního označení nebo ze skutkových okolností, je třeba rozhodnout v každém jednotlivém případě.[223]

218 Rozsudek SDEU ze dne 11. prosince 2014, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, bod 33.

219 Někdejší směrnice 95/46/ES, čl. 3 odst. 2 druhá odrážka, nyní obecné nařízení o ochraně osobních údajů, čl. 2 odst. 2 písm. c).

220 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 7.

221 Modernizovaná úmluva č. 108, čl. 2 písm. d).

222 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 22.

223 Tamtéž.

Příklad: Věc *Google Spain*[224] předložil španělský občan, který chtěl, aby byla z vyhledávače Google odstraněna stará zpráva v novinách o jeho finanční minulosti.

SDEU byla předložena otázka, zda společnost Google jako provozovatel vyhledávače je „správcem" údajů ve smyslu čl. 2 písm. d) směrnice o ochraně údajů.[225] SDEU zvážil širokou definici pojmu „správce" s cílem zajistit „účinn[ou] a úpln[ou] ochran[u] subjektů údajů".[226] SDEU dospěl k závěru, že provozovatel vyhledávače určuje účely a prostředky této činnosti a že zpřístupňuje údaje nahrané na webové stránky vydavateli webových stránek všem internetovým uživatelům, kteří provádějí vyhledávání na základě jména subjektu údajů.[227] Proto SDEU rozhodl, že společnost Google lze považovat za „správce".[228]

Pokud je správce nebo zpracovatel usazen mimo EU, musí tato společnost písemně jmenovat zástupce v EU.[229] GDPR zdůrazňuje, že zástupce musí být usazen „v jednom z členských států, ve kterém se vyskytují subjekty údajů, jejichž osobní údaje jsou zpracovávány v souvislosti s nabízeným zbožím či službami, nebo jejichž chování je monitorováno".[230] I pokud není zástupce jmenován, mohou být zahájeny právní kroky přímo proti správci nebo zpracovateli.[231]

Společní správci

GDPR stanoví, že pokud dva nebo více správců společně určují účel a prostředky zpracování, považují se za společné správce. To znamená, že společně rozhodují o zpracování údajů ke společnému účelu.[232] Vysvětlující zpráva k Modernizované

224 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

225 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 7; Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, bod 21.

226 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, bod 34.

227 Tamtéž, body 35–40.

228 Tamtéž, bod 41.

229 Obecné nařízení o ochraně osobních údajů, čl. 27 odst. 1.

230 Tamtéž, čl. 27 odst. 3.

231 Tamtéž, čl. 27 odst. 5.

232 Tamtéž, čl. 4 bod 7 a článek 26.

úmluvě č. 108 uvádí, že více správců nebo společní správci jsou možní i podle **rámce RE**.[233]

Pracovní skupina zřízená podle článku 29 poukazuje na to, že společné správcovství může mít různé podoby a že účast jednotlivých správců na činnostech souvisejících se správou nemusí být u každého správce stejná.[234] Tato flexibilita umožňuje postihnout stále složitější reálné situace, pokud jde o zpracování údajů.[235] Společní správci proto musí určit svou příslušnou odpovědnost za dodržování povinností stanovených nařízením ve zvláštní dohodě.[236]

Společné správcovství přináší společnou odpovědnost za činnosti zpracování.[237] V rámci **práva EU** to znamená, že každý správce nebo zpracovatel může být plně odpovědný za veškerou újmu způsobenou zpracováním v rámci společného správcovství, aby se zajistila účinná náhrada újmy subjektu údajů.[238]

Příklad: Běžným příkladem společného správcovství je databáze s údaji o zákaznících v prodlení se splácením, kterou provozuje současně několik úvěrových institucí. Pokud někdo požádá některou z bank, která je jedním ze společných správců, o úvěrovou linku, banky nahlédnou do databáze, aby s její pomocí mohly činit informovaná rozhodnutí o úvěruschopnosti žadatele.

Právní ustanovení výslovně neuvádějí, zda společné správcovství vyžaduje, aby byl společný účel pro každého správce totožný, nebo zda stačí, když se jejich účely pouze částečně překrývají. K dnešnímu dni nebyla na evropské úrovni k dispozici žádná příslušná judikatura. Ve svém stanovisku k pojmům správce a zpracovatel z roku 2010 pracovní skupina zřízená podle článku 29 uvedla, že společní správci mohou buď sdílet veškeré účely a prostředky zpracování, nebo mohou sdílet pouze některé účely či prostředky nebo jejich část.[239] Zatímco první uvedený příklad by

233 Modernizovaná úmluva č. 108, čl. 2 písm. d); Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 22.

234 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010, s. 19.

235 Tamtéž.

236 Obecné nařízení o ochraně osobních údajů, 79. bod odůvodnění.

237 Tamtéž, bod 21.

238 Tamtéž, čl. 82 odst. 4.

239 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010, s. 19.

znamenal velmi těsný vztah mezi jednotlivými subjekty, druhý uvedený příklad by svědčil o volnějším vztahu.

Pracovní skupina zřízená podle článku 29 hájí širší výklad pojmu společné správcovství s cílem umožnit určitou flexibilitu za účelem postihnutí stále složitější reálné situace, pokud jde o zpracování údajů.[240] Postoj pracovní skupiny ilustruje věc, do které se zapojila Společnost pro celosvětovou mezibankovní finanční telekomunikaci (SWIFT).

Příklad: V takzvané věci SWIFT využívaly evropské bankovní instituce společnost SWIFT, původně jako zpracovatele, za účelem provádění bankovních převodů při bankovních transakcích. Společnost SWIFT sdělila tyto údaje o bankovních transakcích uložené v počítačovém servisním středisku ve Spojených státech (USA) americkému ministerstvu financí, aniž by jí to výslovně nařídily evropské bankovní instituce, které využívaly jejích služeb. Pracovní skupina zřízená podle článku 29 při posuzování zákonnosti této situace došla k závěru, že evropské bankovní instituce využívající služeb společnosti SWIFT i samotná společnost SWIFT musejí být považovány za společné správce odpovědné evropským zákazníkům za sdělení jejich údajů orgánům USA.[241]

Zpracovatel

Zpracovatele definuje **právo EU** jako osobu, která zpracovává osobní údaje jménem správce.[242] Činnosti svěřené zpracovateli mohou být omezené na velmi konkrétní úkol nebo kontext nebo mohou být poměrně obecné a komplexní.

Podle práva RE je význam pojmu zpracovatel totožný s výkladem podle práva EU.[243]

Zpracovatelé kromě zpracovávání údajů pro jiné osoby budou také sami správci údajů, pokud provádějí zpracování pro své vlastní účely, například, administrativa vlastních zaměstnanců, prodeje a účetnictví.

240 Tamtéž.

241 Pracovní skupina zřízená podle článku 29 (2006), *Stanovisko 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication (SWIFT))*, WP 128, Brusel, 22. listopadu 2006.

242 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 8.

243 Modernizovaná úmluva č. 108, čl. 2 písm. f).

Příklad: Společnost Everready se specializuje na zpracování údajů pro jiné společnosti za účelem správy údajů o lidských zdrojích. Při plnění tohoto úkolu je společnost Everready zpracovatelem. Když však tato společnost zpracovává údaje vlastních zaměstnanců, je správcem operací zpracování údajů za účelem splnění svých povinností zaměstnavatele.

Vztah mezi správcem a zpracovatelem

Jak bylo znázorněno výše, správce je definován jako osoba, která určuje účely a prostředky zpracování. GDPR jasně stanoví, že zpracovatel může zpracovávat osobní údaje pouze na pokyn správce, ledaže zpracování ukládá zpracovateli právo EU nebo členského státu.[244] Smlouva mezi správcem a zpracovatelem je nezbytným prvkem jejich vztahu a jedná se o právní povinnost.[245]

Příklad: Ředitel společnosti Sunshine se rozhodne, že by údaje zákazníků této společnosti měla spravovat společnost Cloudy – specialista na ukládání údajů pomocí cloudové technologie. Společnost Sunshine je i nadále správcem a společnost Cloudy je pouze zpracovatelem, protože podle smlouvy může společnost Cloudy využívat údaje zákazníků společnosti Sunshine pouze k účelům, které určí společnost Sunshine.

Pokud je pravomoc určit prostředky zpracování svěřena zpracovateli, musí správce přesto být schopen vykonávat náležitou úroveň kontroly nad rozhodnutími zpracovatele, pokud jde o prostředky zpracování. Celkovou odpovědnost stále má správce, který musí dohlížet na zpracovatele s cílem zajistit, že jejich rozhodnutí jsou v souladu s právem v oblasti ochrany údajů a s jeho vlastními pokyny.

Kromě toho pokud zpracovatel nedodržuje podmínky pro zpracování údajů stanovené správcem, bude se zpracovatel muset stát správcem alespoň v rozsahu, v jakém porušuje pokyny správce. To s největší pravděpodobností povede k tomu, že se zpracovatel stane nezákonně jednajícím správcem. Naopak původní správce bude muset vysvětlit, jak bylo možné, aby zpracovatel porušil mandát od správce.[246] Pracovní skupina zřízená podle článku 29 skutečně tíhne k tomu, že se v takových

244 Obecné nařízení o ochraně osobních údajů, článek 29.

245 Tamtéž, čl. 28 odst. 3.

246 Tamtéž, čl. 82 odst. 2.

případech jedná o společné správcovství, protože takovýto pohled nabízí nejlepší ochranu zájmů subjektů údajů.[247]

Mohou také vyvstat otázky o rozdělení odpovědnosti, přičemž správce je malý podnik a zpracovatel velká korporátní společnost, která má pravomoc diktovat podmínky ohledně svých služeb. Za těchto okolností však pracovní skupina zřízená podle článku 29 tvrdí, že by standard odpovědnosti neměl být snížen z důvodu hospodářské nerovnováhy a že je třeba zachovat porozumění pojmu správce.[248]

Pro účely jasnosti a transparentnosti musí být zaznamenány podrobnosti vztahu mezi správcem a zpracovatelem v písemné smlouvě.[249] Smlouva musí zahrnovat zejména předmět, povahu, účel a dobu trvání zpracování, typ osobních údajů a kategorie subjektů údajů. Měla by rovněž stanovit povinnosti a práva správce a zpracovatele, například požadavky týkající se důvěrnosti a bezpečnosti. Pokud tato smlouva neexistuje, jedná se o porušení povinnosti správce poskytovat písemnou dokumentaci vzájemných povinností a mohou být za to uloženy sankce. Pokud je újma způsobena v důsledku jednání nad rámec zákonných pokynů správce nebo v rozporu s těmito pokyny, může být právně odpovědný nejen správce, ale také zpracovatel.[250] Zpracovatel musí vést záznamy o všech kategoriích činností zpracování, které provádí jménem správce.[251] Tyto záznamy je třeba na požádání zpřístupnit dozorovému orgánu, protože správce i zpracovatel musí spolupracovat s tímto orgánem při plnění jeho úkolů.[252] Správci a zpracovatelé mají rovněž možnost postupovat podle schváleného kodexu chování nebo mechanismu pro vydávání osvědčení, a tak prokázat, že jednají v souladu s požadavky GDPR.[253]

Zpracovatelé mohou chtít předat některé úkoly dalším zpracovatelům. To je právně přípustné, pokud jsou stanoveny vhodná smluvní ustanovení mezi správcem a zpracovatelem, včetně toho, zda je nezbytné povolení správce v každém jednotlivém

247 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010, s. 25; Pracovní skupina zřízená podle článku 29 (2006), *Stanovisko 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication (SWIFT))*, WP 128, Brusel, 22. listopadu 2006.

248 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010, s. 26.

249 Obecné nařízení o ochraně osobních údajů, čl. 28 odst. 3 a 9.

250 Tamtéž, čl. 82 odst. 2.

251 Tamtéž, čl. 30 odst. 2.

252 Tamtéž, čl. 30 odst. 4 a článek 31.

253 Tamtéž, čl. 28 odst. 5 a čl. 42 odst. 4.

případě nebo zda je dostatečné pouhé informování. GDPR stanoví, že neplní-li další zpracovatel své povinnosti v oblasti ochrany údajů, nese právní odpovědnost nadále plně prvotní zpracovatel.[254]

Podle práva RE se plně uplatní výklad pojmů správce a zpracovatel, jak je vysvětleno výše.[255]

2.3.2. Příjemci a třetí strany

Rozdíl mezi těmito dvěma kategoriemi osob nebo subjektů, které byly zavedeny směrnicí o ochraně údajů, spočívá hlavně v jejich vztahu ke správci, a tudíž v jejich povolení získat přístup k osobním údajům v držení správce.

„Třetí strana" je osoba, která je odlišná od správce a zpracovatele. Podle čl. 4 bodu 10 GDPR je třetí strana „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů". To znamená, že osoby pracující pro organizaci, která není totožná se správcem – i když patří do téže skupiny nebo holdingu –, budou „třetí stranou" (nebo k ní budou přináležet). Na druhou stranu nebudou „třetí stranou" pobočky jedné banky zpracovávající účty zákazníků pod přímým dohledem jejich ústředí.[256]

„Příjemce" je širší pojem než „třetí strana". Ve smyslu čl. 4 bodu 9 GDPR se příjemcem rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli". Tímto příjemcem může být buď osoba, která není správcem nebo zpracovatelem ani jejich součástí, – ta by pak byla třetí stranou – nebo někdo v rámci správce nebo zpracovatele, například zaměstnanec nebo jiné oddělení v rámci téže společnosti nebo orgánu.

Rozdíl mezi příjemci a třetími stranami je důležitý pouze kvůli podmínkám pro zákonné předávání údajů. Zaměstnanci správce nebo zpracovatele mohou být příjemci osobních údajů bez dalších právních požadavků, pokud se podílejí na operacích zpracování prováděných správcem nebo zpracovatelem. Naproti tomu třetí strana, která je oddělená od správce nebo zpracovatele, není oprávněna používat osobní

254 Tamtéž, čl. 28 odst. 4.

255 Viz například Modernizovanou úmluvu č. 108 čl. 2 písm. b) a f); doporučení o profilování, článek 1.

256 Pracovní skupina zřízená podle článku 29 (2010), *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"*, WP 169, Brusel, 16. února 2010, s. 31.

údaje, které zpracovává správce, s výjimkou zvláštních právních důvodů ve specifických případech.

Příklad: Zaměstnanec správce, který používá osobní údaje v rámci provádění úkolů, kterými ho pověřil zaměstnavatel, je příjemcem údajů, ale nikoliv třetí stranou, protože používá údaje jménem správce a podle jeho pokynů. Například pokud zaměstnavatel předá osobní údaje o svých zaměstnancích personálnímu oddělení s ohledem na nadcházející hodnocení výkonnosti zaměstnanců, tým lidských zdrojů bude příjemcem osobních údajů, protože údaje jim byly předány v průběhu zpracování prováděného ve prospěch správce.

Pokud však organizace poskytne údaje o svých zaměstnancích školicí společnosti, která je bude používat k upravení programu školení na míru těmto zaměstnancům, je tato školicí společnost třetí stranou. Důvodem je, že školicí společnost nemá zvláštní legitimitu nebo povolení (které v případě, kdy šlo o „personální oddělení", vyplývá ze zaměstnaneckého vztahu se správcem) ke zpracování těchto osobních údajů. Jinými slovy: neobdrželi informace během doby svého zaměstnání u správce údajů.

2.4. Souhlas

Hlavní body

- Souhlas jako právní základ pro zpracování osobních údajů musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle formou zjevného potvrzení svolení ke zpracování.
- Zpracování zvláštních kategorií údajů vyžaduje výslovný souhlas.

Jak bude důkladně pojednáno v kapitole 4, souhlas je jedním ze šesti legitimních důvodů pro zpracování osobních údajů. Souhlasem se rozumí „jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle"[257] subjektu údajů.

257 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 11. Viz také Modernizovanou úmluvu č. 108, čl. 5 odst. 2.

Právo EU stanoví několik prvků, které musí souhlas mít, aby byl platný. Cílem těchto prvků je pak zaručit, že subjekty údajů myslely vážně svůj souhlas s konkrétním využitím svých údajů:[258]

- Souhlas musí být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování svých osobních údajů. Může mít podobu činnosti nebo prohlášení.

- Subjekt údajů musí mít právo kdykoliv souhlas odvolat.

- V kontextu písemného prohlášení, které také zahrnuje jiné záležitosti, např. „podmínky poskytování služeb", musí být žádosti o souhlas uvedeny jasnými a jednoduchými jazykovými prostředky ve srozumitelném a snadno přístupném znění, které jasně odlišuje souhlas od jiných záležitostí; pokud některá část tohoto prohlášení je v rozporu s GDPR, není závazná.

Souhlas může být v kontextu práva na ochranu údajů platný pouze tehdy, pokud jsou splněny všechny tyto požadavky. Je povinností správce prokázat, že subjekt údajů udělil souhlas se zpracováním svých údajů.[259] Prvky platného souhlasu budou pojednány níže v oddílu 4.1.1 o zákonných důvodech pro zpracování osobních údajů.

Úmluva č. 108 neobsahuje definici souhlasu, její vymezení je ponecháno na vnitrostátním právu. Avšak **podle práva RE** prvky platného souhlasu odpovídají těm, které byly objasněny výše.[260]

Další požadavky týkající se platného souhlasu podle občanského práva, například způsobilost k právům a právním úkonům, pochopitelně platí i v souvislosti s ochranou údajů, protože tyto požadavky jsou základními právními předpoklady. Neplatný souhlas osob, které nemají způsobilost k právům a právním úkonům, bude mít za následek absenci právního základu pro zpracování údajů o těchto osobách. Pokud jde o způsobilost k právům a právním úkonům nezletilých osob s ohledem na uzavírání smluv, GDPR stanoví, že pravidly pro minimální věk, kdy lze získat platný souhlas, není dotčeno obecné smluvní právo členských států.[261]

258 Obecné nařízení o ochraně osobních údajů, článek 7.

259 Tamtéž, čl. 7 odst. 1.

260 Modernizovaná úmluva č. 108, čl. 5 odst. 2; Vysvětlující zpráva k Modernizované úmluvě č. 108, body 42–45.

261 Obecné nařízení o ochraně osobních údajů, čl. 8 odst. 3.

Souhlas musí být udělen jasným způsobem, aby se vyloučily veškeré pochybnosti o záměru subjektu údajů.[262] Souhlas musí být výslovný, pokud jde o zpracování citlivých osobních údajů, a je možné jej poskytnout ústně nebo písemně.[263] Písemný souhlas lze udělit i elektronicky.[264] V rámci **práva EU** i **RE** musí být souhlas se zpracováním vlastních osobních údajů udělen prohlášením nebo jednoznačným potvrzením.[265] Souhlas tudíž nelze vyvodit z mlčení, předem zaškrtnutých políček, předvyplněných formulářů nebo nečinnosti.[266]

262 Tamtéž, čl. 6 odst. 1 písm. a) a čl. 9 odst. 2 písm. a).

263 Tamtéž, 32. bod odůvodnění.

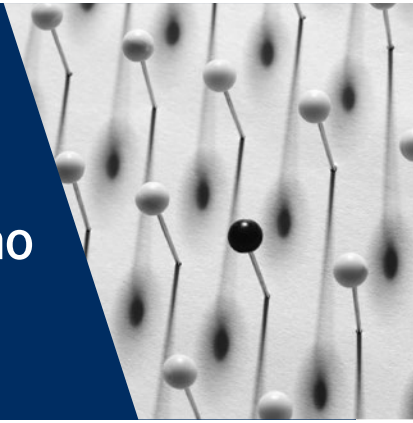
264 Tamtéž.

265 Tamtéž, čl. 4 bod 11; Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 42.

266 Viz obecné nařízení o ochraně osobních údajů, 32. bod odůvodnění; Vysvětlující zprávu k Modernizované úmluvě č. 108, bod 42.

3

Hlavní zásady evropského práva v oblasti ochrany údajů



EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a)	**Zásada zákonnosti**	Modernizovaná úmluva č. 108, čl. 5 odst. 3
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a)	**Zásada korektnosti**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. a) Rozsudek ESLP z roku 2009, *K. H. a další v. Slovensko*, č. 32881/04
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a) Rozsudek SDEU z roku 2015, C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*	**Zásada transparentnosti**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. a) a článek 8 Rozsudek ESLP ze dne 2009, *Haralambie v. Rumunsko*, č. 21737/03
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. b)	**Zásada účelového omezení**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b)
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. c) Rozsudek SDEU (velkého senátu) z roku 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland a Kärntner Landesregierung a další*	**Zásada minimalizace údajů**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. c)

EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. d) Rozsudek SDEU z roku 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*	**Zásada přesnosti údajů**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. d)
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. e) Rozsudek SDEU (velkého senátu) z roku 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland a Kärntner Landesregierung a další*	**Zásada omezení uložení**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. e) Rozsudek ESLP (velkého senátu) z roku 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. f) a článek 32	**Zásada zabezpečení údajů (integrita a důvěrnost)**	Modernizovaná úmluva č. 108, článek 7
Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 2	**Zásada odpovědnosti**	Modernizovaná úmluva č. 108, článek 10

Článek 5 obecného nařízení o ochraně osobních údajů stanoví zásady, kterými se řídí zpracování osobních údajů. K těmto zásadám patří:

- zákonnost, korektnost a transparentnost,
- účelové omezení,
- minimalizace údajů,
- přesnost údajů,
- omezení uložení,
- integrita a důvěrnost.

Zásady jsou východiskem pro podrobnější ustanovení uvedená v níže uvedených článcích nařízení. Objevují se také v článcích 5, 7, 8 a 10 Modernizované úmluvy č. 108. Veškeré pozdější právní předpisy na úrovni EU či RE v oblasti ochrany údajů

musejí být v souladu s těmito zásadami a je třeba je mít na paměti při výkladu těchto právních předpisů. Podle práva EU jsou omezení zásad zpracování možná pouze v rozsahu, v jakém odpovídají právům a povinnostem stanoveným v článcích 12 až 22, a musejí dodržovat podstatu základních práv a svobod. Na úrovni EU nebo na vnitrostátní úrovni mohou být stanoveny výjimky a omezení týkající se těchto hlavních zásad;[267] musejí být stanoveny zákonem, sledovat legitimní cíl a představovat nezbytné a přiměřené opatření v demokratické společnosti. [268] Musejí být splněny všechny tři podmínky.

3.1. Zásady zpracování: zákonnost, korektnost a transparentnost

Hlavní body

- Zásady zákonnosti, korektnosti a transparentnosti se použijí na zpracování všech osobních údajů.
- Podle GDPR je podmínkou zákonnosti splnění nejméně jednoho z uvedených bodů:
  - souhlas subjektu údajů,
  - nezbytnost pro uzavření smlouvy,
  - právní povinnost,
  - nezbytnost pro ochranu životně důležitých zájmů subjektu údajů nebo jiné osoby,
  - nezbytnost pro splnění úkolu prováděného ve veřejném zájmu,
  - nezbytnost pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy a práva subjektu údajů.
- Zpracování osobních údajů je třeba provádět korektně.
  - Subjekt údajů musí být informován o riziku, aby bylo zajištěno, že zpracování nemá nepředvídané nežádoucí účinky.

267 Modernizovaná úmluva č. 108, čl. 11 odst. 1; obecné nařízení o ochraně osobních údajů, čl. 23 odst. 1.

268 Obecné nařízení o ochraně osobních údajů, čl. 23 odst. 1.

- Zpracování osobních údajů je třeba provádět transparentně.
  - Správci musí informovat subjekty údajů, než začnou zpracovávat jejich údaje, mimo jiné pak o účelu zpracování a o totožnosti a adrese správce.
  - Informace o operacích zpracování musí být poskytnuty za použití jasných a jednoduchých jazykových prostředků, aby subjekty údajů mohly snadno porozumět příslušným pravidlům, rizikům, zárukám a právům.
  - Subjekty údajů mají vždy právo na přístup ke svým zpracovávaným údajům.

3.1.1. Zákonnost zpracování

Právní předpisy EU a RE v oblasti ochrany údajů vyžadují zákonné zpracování osobních údajů.[269] K zákonnému zpracování je zapotřebí souhlasu subjektu údajů nebo jiný oprávněný důvod stanovený v právních předpisech o ochraně údajů.[270] Článek 6 odst. 1 GDPR obsahuje pět zákonných důvodů pro zpracování kromě souhlasu, tj. když je zpracování osobních údajů nezbytné pro splnění smlouvy, pro splnění úkolu prováděného při výkonu veřejné moci, pro splnění právní povinnosti, pro účely oprávněných zájmů správce či třetí strany nebo pro ochranu životně důležitých zájmů subjektu údajů. O tom podrobněji pojednává oddíl 4.1.

3.1.2. Korektnost zpracování

Právní předpisy EU a RE v oblasti ochrany údajů vyžadují kromě zákonnosti zpracování osobních údajů také to, aby údaje byly zpracovávány korektně.[271] Zásada korektního zpracování se týká především vztahu mezi správcem a subjektem údajů.

Správci by měli informovat subjekty údajů a širokou veřejnost o tom, že budou zpracovávat údaje zákonným a transparentním postupem, a musejí být schopni prokázat soulad operací zpracování s GDPR. Operace zpracování nesmí být prováděny tajně a subjekty údajů by si měly být vědomy možných rizik. Kromě toho musí správci v maximálním možném rozsahu jednat tak, aby neprodleně vyhověli přáním subjektu údajů, zejména pokud jeho souhlas je právním základem zpracování údajů.

269 Modernizovaná úmluva č. 108, čl. 5 odst. 3; obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a).

270 Listina základních práv Evropské unie, čl. 8 odst. 2; obecné nařízení o ochraně osobních údajů, 40. bod odůvodnění a články 6–9; Modernizovaná úmluva č. 108, čl. 5 odst. 2; Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 41.

271 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. a).

Příklad: Ve věci *K. H. a další v. Slovensko*[272] stěžovatelky – ženy romské národnosti – pobývaly během těhotenství a porodu ve dvou nemocnicích na východním Slovensku. Následně žádná z nich nedokázala znovu počít dítě navzdory opakovaným pokusům. Vnitrostátní soudy vydaly nemocnicím příkaz, aby umožnily stěžovatelkám a jejich zástupcům nahlédnout do lékařských záznamů a pořídit z nich ručně psaný výtah, ale zamítly jejich žádost o pořízení fotokopií těchto dokumentů, a to údajně proto, aby zabránily jejich zneužití. Pozitivní povinnost států uvedená v článku 8 EÚLP nutně zahrnuje povinnost zpřístupnit subjektům údajů kopie spisů s jejich údaji. Je věcí státu určit, za jakých podmínek bude možné pořídit kopie spisů s osobními údaji nebo případně prokázat přesvědčivé důvody vedoucí k zamítnutí tohoto požadavku. V případě stěžovatelek vnitrostátní soudy odůvodnily zákaz, aby stěžovatelky pořizovaly kopie svých lékařských záznamů, především nutností ochránit příslušné informace před zneužitím. ESLP však nerozuměl tomu, jak by stěžovatelky, které již tak jako tak získaly přístup k úplným lékařským záznamům, mohly zneužít informace týkající se jich samotných. Kromě toho bylo možné zabránit riziku takového zneužití jinými prostředky, než je odepření možnosti pořídit kopie ze spisů stěžovatelek, například omezením okruhu osob, které by měly právo nahlédnout do spisů. Stát neprokázal existenci dostatečně přesvědčivých důvodů pro to, aby odepřel stěžovatelkám účinný přístup k informacím o jejich zdraví. Soud rozhodl, že došlo k porušení článku 8.

V souvislosti s internetovými službami musí prvky systémů pro zpracování údajů subjektům údajů umožňovat, aby skutečně porozuměly tomu, co se děje s jejich údaji. V každém případě překračuje zásada korektnosti povinnosti v oblasti transparentnosti a může být rovněž dávána do souvislosti s etikou zpracování osobních údajů.

Příklad: Výzkumné oddělení jedné univerzity provádí experiment, při kterém analyzuje změny nálad u 50 subjektů. Tyto subjekty musejí každou hodinu v daném čase zaznamenávat do elektronické evidence své myšlenky. Těchto 50 osob udělilo souhlas pro tento konkrétní projekt a toto konkrétní užití údajů ze strany univerzity. Výzkumné oddělení brzy zjistí, že elektronicky zaznamenané myšlenky by byly velmi užitečné pro jiný projekt zkoumající duševní zdraví, který koordinuje jiný tým. Ačkoliv univerzita by jako správce

272 Rozsudek ESLP ze dne 28. dubna 2009, *K. H. a další v. Slovensko*, č. 32881/04.

mohla využít tytéž údaje pro činnost jiného týmu bez dalších kroků k zajištění zákonnosti zpracování těchto údajů vzhledem k tomu, že účely jsou slučitelné, univerzita informovala subjekty a požádala je o nový souhlas v souladu s etickým kodexem výzkumu a zásadou korektního zpracování.

3.1.3. Transparentnost zpracování

Právní předpisy EU a RE v oblasti ochrany údajů vyžadují, aby se zpracování osobních údajů provádělo „ve vztahu k subjektu údajů [...] korektně a zákonným a transparentním způsobem".[273]

Tato zásada stanoví povinnost správce přijmout veškerá vhodná opatření s cílem zajistit informovanost subjektů údajů – může jít o uživatele, zákazníky nebo klienty – o tom, jak jsou jejich údaje používány.[274] Transparentností se mohou rozumět informace poskytnuté jednotlivci před zahájením zpracování,[275] informace, které by měly být snadno přístupné subjektům údajů během zpracování,[276] ale také informace poskytnuté subjektům údajů v návaznosti na žádost o přístup k vlastním údajům.[277]

Příklad: Ve věci *Haralambie v. Rumunsko*[278] byl stěžovateli poskytnut přístup k informacím, kterými o něm disponovala organizace tajných služeb, až pět let od podání žádosti. ESLP zopakoval, že jednotlivci, jejichž informace jsou obsaženy v osobních složkách v držení veřejných orgánů, mají zásadní zájem na tom, aby k nim měli přístup. Orgány mají povinnost zajistit účinný postup pro získání přístupu k těmto informacím. ESLP se domníval, že ani množství předaných spisů, ani nedostatky archivního systému neodůvodňují pětileté zpoždění, pokud jde o vyhovění žádosti stěžovatele o přístup ke své složce. Orgány musí zajistit stěžovateli účinný a dostupný postup, který mu umožní získat přístup k osobním spisům v rozumné lhůtě. Soud rozhodl, že došlo k porušení článku 8 EÚLP.

273 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. a); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. a) a článek 8.

274 Obecné nařízení o ochraně osobních údajů, článek 12.

275 Tamtéž, článek 13 a 14.

276 Pracovní skupina zřízená podle článku 29, *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti*, s. 23.

277 Obecné nařízení o ochraně osobních údajů, článek 15.

278 Rozsudek ESLP ze dne 27. října 2009, *Haralambie v. Rumunsko*, č. 21737/03.

Operace zpracování musí být subjektům údajů vysvětleny snadno přístupným způsobem, což zajistí, že porozumí tomu, co se stane s jejich údaji. To znamená, že konkrétní účel zpracování osobních údajů musí být subjektu údajů znám v okamžiku shromažďování osobních údajů.[279] Aby bylo zpracování transparentní, je nutné, aby byly použity jasné a jednoduché jazykové prostředky.[280] Dotčeným osobám musí být jasné, jaká jsou rizika, pravidla, záruky a práva týkající se zpracování jejich osobních údajů.[281]

Právo RE rovněž upřesňuje, že některé nezbytné informace musí správce povinně aktivně poskytovat subjektům údajů. Informace o jménu (názvu) a adrese správce (nebo společných správců), právní základ a účely zpracování údajů, kategorie zpracovávaných údajů a příjemci, jakož i prostředky výkonu práv mohou být stanoveny ve vhodném formátu (prostřednictvím webové stránky, technologických nástrojů na osobních zařízeních atd.), pokud jsou informace korektně a účinně předkládány subjektu údajů. Předložené informace by měly být snadno přístupné, čitelné, srozumitelné a přizpůsobené příslušným subjektům údajů (například v jazyce srozumitelném dětem, je-li to nutné). Také je třeba poskytnout veškeré další informace, které jsou nezbytné k zajištění korektního zpracování údajů nebo které jsou k takovému účelu užitečné, například doba uchovávání, znalosti o důvodech pro zpracování údajů nebo informace o předávání údajů příjemci v jiné smluvní straně nebo v zemi, která není smluvní stranou (včetně toho, zda daná země, která není smluvní stranou, zajišťuje vhodnou úroveň ochrany nebo zda správcem přijatá opatření zaručují tuto vhodnou úroveň ochrany údajů). [282]

V souladu s právem na přístup k osobním údajům[283] má subjekt údajů právo, aby mu správce na jeho žádost sdělil, zda zpracovává jeho údaje, a pokud ano, které údaje jsou předmětem takového zpracování.[284] Kromě toho v souladu s právem na informace[285] musí být osoby, jejichž údaje se zpracovávají, aktivně informovány správci nebo zpracovateli mimo jiné o účelu, délce trvání a prostředcích zpracování, a to v zásadě před zahájením zpracovávání údajů.

279 Obecné nařízení o ochraně osobních údajů, 39. bod odůvodnění.

280 Tamtéž.

281 Tamtéž.

282 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 68.

283 Obecné nařízení o ochraně osobních údajů, článek 15.

284 Modernizovaná úmluva č. 108, článek 8 a čl. 9 odst. 1 písm. b).

285 Obecné nařízení o ochraně osobních údajů, článek 13 a 14.

Příklad: Věc *Smaranda Bara a další v. Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] se týkala předávání daňových údajů týkajících se příjmu osob samostatně výdělečně činných ze strany Státní agentury pro správu daní a poplatků Státnímu fondu sociálního zabezpečení v Rumunsku. Na základě těchto údajů pak byly požadovány úhrady nedoplatků na příspěvcích na zdravotní pojištění. SDEU byl požádán, aby rozhodl, zda měl být subjekt údajů předem informován o totožnosti správce údajů a o účelu předání těchto údajů, než byly tyto údaje zpracovány Státním fondem sociálního zabezpečení. SDEU rozhodl, že pokud orgán veřejné správy členského státu předává osobní údaje jinému orgánu veřejné správy, který tyto údaje následně zpracovává, musí být subjekty údajů o tomto předání nebo zpracování informovány.

V některých situacích jsou možné odchylky od povinnosti informovat subjekty údajů o zpracování údajů a o těchto odchylkách pojednává podrobněji oddíl 6.1 o právech subjektu údajů.

3.2. Zásada účelového omezení

Hlavní body

- Účel zpracování údajů musí být definován před zahájením zpracovávání.
- Není možné dále zpracovávat údaje způsobem, který je neslučitelný s původním účelem, ačkoliv obecné nařízení o ochraně osobních údajů stanoví výjimky z tohoto pravidla pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu a pro statistické účely.
- Zásada účelového omezení v podstatě znamená, že veškeré zpracovávání osobních údajů musí probíhat za určitým, řádně definovaným účelem a v případě dodatečných, upřesněných účelů pouze tehdy, pokud jsou slučitelné s původním účelem.

Zásada účelového omezení je jednou ze základních zásad evropského práva v oblasti ochrany údajů. Je silně provázána s transparentností, předvídatelností a uživatelskou kontrolou: pokud účel zpracování je dostatečně konkrétní a jednoznačný, jednotlivci vědí, co mohou očekávat, a zvýší se transparentnost a právní jistota. Současně je jasné vymezení účelů důležité k tomu, aby umožnilo subjektům údajů

286 Rozsudek SDEU ze dne 1. října 2015, C-201/14, *Smaranda Bara a další v. Casa Naţională de Asigurări de Sănătate a další*, body 28–46.

účinně vykonávat svá práva, například právo vznést námitku proti zpracování osobních údajů.[287]

Zásada ukládá, aby veškeré zpracovávání osobních údajů probíhalo za určitým, řádně definovaným účelem a v případě dodatečných účelů pouze tehdy, pokud jsou slučitelné s původním účelem.[288] Zpracování osobních údajů pro nedefinované a/nebo neomezené účely je tudíž protiprávní. Zpracování osobních údajů bez určitého účelu, pouze na základě úvahy, že mohou být někdy v budoucnu užitečné, také není v souladu s předpisy. Legitimita zpracovávání osobní údajů bude záviset na účelu zpracování, který musí být jednoznačný, upřesněný a legitimní.

Každý nový účel zpracování údajů, který není slučitelný s původním účelem, musí mít svůj vlastní zvláštní právní základ a nemůže spoléhat pouze na skutečnost, že údaje byly původně získány nebo zpracovávány za jiným legitimním účelem. Legitimní zpracování je pak omezeno na svůj původně upřesněný účel a každý nový účel zpracování bude vyžadovat samostatný nový právní základ. Například poskytování osobních údajů třetím stranám za novým účelem bude muset být důkladně zváženo, protože toto zveřejnění bude pravděpodobně vyžadovat další právní základ, který je odlišný od základu pro shromažďování údajů.

Příklad: Jistý letecký dopravce shromažďuje údaje od svých cestujících za účelem provádění rezervací a řádného provozování letu. Dopravce bude potřebovat údaje o: číslech sedadel cestujících, zvláštních tělesných omezeních, například o potřebě zajistit invalidní vozík, a o zvláštních požadavcích na stravu, např. košer nebo halal potraviny. Pokud budou letečtí dopravci požádáni o předání těchto údajů, které jsou obsaženy ve jmenné evidenci cestujících, imigračním orgánům v místě přistání, budou tyto údaje následně použity pro účely imigrační kontroly, které jsou odlišné od původního účelu shromažďování údajů. Předání těchto údajů imigračním orgánům bude tedy vyžadovat nový a samostatný právní základ.

Při zvažování oblasti působnosti a mezí konkrétního účelu vychází Modernizovaná úmluva č. 108 a obecné nařízení o ochraně osobních údajů z pojmu slučitelnosti: používání údajů pro účely slučitelnosti je povoleno na původním právním základě. Další zpracování údajů proto nesmí být provedeno způsobem, který subjekt údajů

287 Pracovní skupina zřízená podle článku 29 (2013), *Stanovisko 3/2013 k účelovému omezení*, WP 203, Brusel, 2. dubna 2013.

288 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. b).

neočekává, který je nevhodný nebo nepřijatelný.[289] Při posuzování, zda je dané zpracování třeba považovat za slučitelné, by správce měl (kromě jiného) zohlednit tyto body:

- „jakoukoliv vazbu mezi těmito účely a účely zamýšleného dalšího zpracování,
- kontext, v němž byly osobní údaje shromážděny, zejména přiměřená očekávání ohledně dalšího použití osobních údajů, která mají subjekty údajů na základě svého vztahu se správcem,
- povahu osobních údajů,
- důsledky zamýšleného dalšího zpracování pro subjekty údajů a
- existenci vhodných záruk jak během původních, tak během zamýšlených dalších operací zpracování.“[290] To lze provést například prostřednictvím šifrování nebo pseudonymizace.

Příklad: Společnost Sunshine získává údaje zákazníků v rámci řízení vztahů se zákazníky (CRM). Následně tyto údaje předává společnosti Moonlight zabývající se přímým marketingem, jež chce tyto údaje využít k tomu, aby mohla pomoci třetím společnostem v marketingových kampaních. Pokud společnost Sunshine předává údaje pro účely marketingu prováděného jinými společnostmi, jedná se o následné použití údajů k novému účelu, který je neslučitelný s CRM, což je původní účel společnosti Sunshine pro shromažďování údajů o zákaznících. Předání údajů společnosti Moonlight proto vyžaduje vlastní právní základ.

Naopak používání údajů získaných v rámci CRM společnosti Sunshine pro vlastní marketingové účely, tj. zasílání marketingových sdělení vlastním zákazníkům týkajících se vlastních produktů společnosti, se obecně chápe jako slučitelný účel.

289 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 49.

290 Viz obecné nařízení o ochraně osobních údajů, 50. bod odůvodnění a čl. 6 odst. 4; Vysvětlující zprávu k Modernizované úmluvě č. 108, bod 49.

Obecné nařízení o ochraně osobních údajů a Modernizovaná úmluva č. 108 uvádí, že „další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely" je *a priori* považováno za slučitelné s původním účelem.[291] Při dalším zpracovávání osobních údajů je však třeba zavést vhodné záruky, jako je anonymizace, šifrování nebo pseudonymizace údajů a omezení přístupu k údajům.[292] V obecném nařízení o ochraně osobních údajů se dodává, že „[p]okud subjekt údajů udělil souhlas nebo pokud je zpracování na základě práva Unie nebo členského státu, které představuje v rámci demokratické společnosti nezbytné a přiměřené opatření s cílem zajistit zejména důležité cíle obecného veřejného zájmu, měl by správce mít možnost dalšího zpracování osobních údajů bez ohledu na slučitelnost účelů".[293] Při provádění dalšího zpracovávání by tedy subjekt údajů měl být informován o účelech i o svých právech, například právu vznést námitku.[294]

Příklad: Společnost Sunshine shromažďuje a ukládá údaje od svých zákazníků v souvislosti s řízením vztahů se zákazníky (CRM). Další používání těchto údajů společností Sunshine za účelem statistické analýzy nákupního chování jejích zákazníků je přípustné, protože statistika je slučitelný účel. Není zapotřebí žádný další právní základ, např. souhlas subjektů údajů. Avšak k dalšímu zpracování osobních údajů pro statistické účely musí společnost Sunshine zavést vhodné záruky práv a svobod subjektu údajů. K technickým a organizačním opatřením, která musí společnost Sunshine zavádět, může patřit i pseudonymizace.

291 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. b); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b). Příkladem takovýchto vnitrostátních ustanovení je rakouský zákon o ochraně údajů (*Datenschutzgesetz*), Bundesgesetzblatt I č. 165/1999, bod 46.

292 Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 4; Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b); Vysvětlující zprávu k Modernizované úmluvě č. 108, bod 50.

293 Obecné nařízení o ochraně osobních údajů, 50. bod odůvodnění.

294 Tamtéž.

3.3. Zásada minimalizace údajů

Hlavní body

- Zpracování údajů musí být omezeno na to, co je nezbytné ke splnění legitimního účelu.
- Ke zpracování osobních údajů by mělo dojít pouze tehdy, když účelu zpracování nelze rozumně dosáhnout jinými prostředky.
- Zpracování údajů nesmí nepřiměřeně zasahovat do dotčených zájmů, práv a svobod.

Lze zpracovávat pouze ty údaje, které jsou „přiměřené, relevantní a nepřekračují nezbytný rozsah ve vztahu k účelu, pro který jsou shromažďovány a/nebo dále zpracovávány".[295] Kategorie údajů, které byly vybrány ke zpracování, musí být nezbytné k dosažení uváděného celkového cíle operací zpracování a správce by měl důsledně omezit shromažďování údajů na takové informace, které jsou přímo relevantní pro konkrétní účel, který zpracování sleduje.

Příklad: Ve věci *Digital Rights Ireland*[296] SDEU posuzoval platnost směrnice o uchovávání údajů, jejímž cílem bylo harmonizovat vnitrostátní ustanovení pro uchovávání osobních údajů vytvářených nebo zpracovávaných veřejně dostupnými službami nebo sítěmi elektronických komunikací za účelem možného předání příslušným orgánům s cílem bojovat proti závažným trestným činům, jako je organizovaná trestná činnost a terorismus. Bez ohledu na to, že se soud domníval, že se jedná o účel, který skutečně odpovídá cíli obecného zájmu, zevšeobecnění, podle kterého se směrnice vztahuje na „každou osobu, každý prostředek elektronické komunikace a na všechny provozní údaje bez jakéhokoli rozlišování, omezení či výjimky v závislosti na cíli boje proti závažné trestné činnosti", byl shledán problematickým.[297]

Kromě toho prostřednictvím využití zvláštní technologie na zvýšení soukromí je někdy možné úplně předejít využívání osobních údajů nebo používat opatření ke

295 Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. c); obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. c).

296 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

297 Tamtéž, body 44 a 57.

snížení schopnosti přiřadit údaje danému subjektu údajů (například prostřednictvím pseudonymizace), což přináší řešení, které je vstřícné k ochraně soukromí. To je vhodné zejména v rozsáhlejších systémech zpracování.

Příklad: Městská rada nabízí pravidelným uživatelům městského systému veřejné hromadné dopravy za určitý poplatek čipovou kartu. Karta obsahuje jméno uživatele v písemné podobě na povrchu karty a rovněž v elektronické podobě v čipu. Při každé jízdě autobusem nebo tramvají je nutné přiložit čipovou kartu ke čtečce nainstalované například přímo v autobusech a v tramvajích. Údaje, které toto zařízení načte, jsou elektronicky porovnány s databází obsahující jména osob, které si zakoupily přepravní kartu.

Tento systém není v optimálním souladu se zásadou minimalizace údajů: ověřování, zda má jednotlivec oprávnění používat dopravní prostředky, by mohlo být prováděno tak, aniž by byly porovnávány osobní údaje na čipu karty s databází. Stačilo by například mít zvláštní elektronický obrázek, jako je čárový kód, na čipu karty, který by při přiložení ke čtecímu zařízení potvrdil, zda je karta platná. Takový systém by nezaznamenával, kdo kdy použil jaký dopravní prostředek. Jednalo by se o optimální řešení ve smyslu zásady minimalizace, protože tato zásada přináší povinnost minimalizovat shromažďování údajů.

Článek 5 odst. 1 Modernizované úmluvy č. 108 obsahuje požadavek přiměřenosti pro zpracování osobních údajů týkající se sledovaného legitimního účelu. Musí být dosaženo spravedlivé rovnováhy mezi všemi dotčenými zájmy ve všech fázích zpracovávání. To znamená, že „[o]sobní údaje, které jsou odpovídající a relevantní, ale zahrnovaly by nepřiměřený zásah do dotčených základních práv a svobod, je třeba považovat za nepřiměřené“.[298]

298 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 52; obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. c).

3.4. Zásada přesnosti údajů

Hlavní body

- Zásadu přesnosti údajů musí správce provádět ve všech operacích zpracování.
- Nepřesné údaje musí být neprodleně smazány nebo opraveny.
- Pro zajištění přesnosti může být nutné údaje pravidelně kontrolovat a aktualizovat.

Správce, který má v držení osobní informace, nesmí tyto informace použít, aniž by podnikl kroky k zajištění, že údaje jsou s rozumnou mírou jistoty přesné a aktualizované.[299]

Na povinnost zajišťovat přesnost údajů je třeba nahlížet v souvislosti s účelem zpracování údajů.

Příklad: Ve věci *Rijkeboer*[300] SDEU projednával žádost nizozemského státního příslušníka o informace od místní správy města Amsterdamu o totožnosti osob, jímž byly v uplynulých dvou letech předány záznamy o něm v držení místní správy, a také o obsahu předaných údajů. SDEU uvedl, že „právo na respektování soukromí předpokládá, že se subjekt údajů může ujistit, zda jsou jeho osobní údaje zpracovávány bezchybně a přípustným způsobem, což zejména znamená, že jsou základní údaje, jež se jej týkají, správné a že jsou určeny oprávněným příjemcům“. SDEU pak odkázal na preambuli směrnice o ochraně údajů, v níž se uvádí, že subjekty údajů musí požívat práva na přístup ke svým osobním údajům, aby se mohly přesvědčit o jejich přesnosti.[301]

Mohou rovněž nastat případy, kdy aktualizace uložených údajů je zakázána právními předpisy, protože účelem ukládání údajů je především dokumentovat události jako zachycení momentální historické situace.

299 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. d); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. d).

300 Rozsudek SDEU ze dne 7. května 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*.

301 Někdejší 41. bod odůvodnění, preambule směrnice 95/46/ES.

Příklad: Lékařské záznamy o operaci nesmí být měněny, jinými slovy „aktualizovány“, i když nálezy uvedené v záznamech se později ukáží jako nesprávné. Za těchto okolností lze pouze vložit doplnění k poznámkám v záznamech, pokud jsou tato doplnění jasně označena jako pozdější příspěvky.

Na druhou stranu nastávají situace, kdy je naprosto nezbytné aktualizovat a pravidelně kontrolovat přesnost údajů kvůli možné újmě, kterou by mohly způsobit subjektu údajů, pokud by údaje zůstaly i nadále nepřesné.

Příklad: Pokud chce někdo uzavřít smlouvu o úvěru s bankovní institucí, banka obvykle ověří úvěruschopnost potenciálního zákazníka. Za tímto účelem jsou k dispozici zvláštní databáze obsahující údaje o úvěrové historii soukromých osob. Pokud jsou v této databázi uvedeny nesprávné nebo zastaralé údaje o takové osobě, může to pro ni mít nepříznivé důsledky. Správci těchto databází proto musí vyvinout zvláštní úsilí, aby se řídili zásadou přesnosti.

3.5. Zásada omezení uložení

Hlavní body

- Zásada omezení uložení znamená, že osobní údaje musí být smazány nebo anonymizovány, jakmile již nejsou zapotřebí pro účely, ke kterým byly shromážděny.

Článek 5 odst. 1 písm. e) GDPR a podobně čl. 5 odst. 4 písm. e) Modernizované úmluvy č. 108 vyžadují, aby osobní údaje byly „uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které“ jsou zpracovávány. Jakmile tedy údaje posloužily těmto účelům, musí být smazány nebo anonymizovány. Proto by měl „správce stanovit lhůty pro výmaz nebo pravidelný přezkum“, aby bylo zajištěno, že údaje nebudou uchovávány déle, než je nezbytné.[302]

ESLP ve věci *S. a Marper* rozhodl, že hlavní zásady příslušného nástroje Rady Evropy a právo a praxe ostatních smluvních stran ukládají, aby uchovávání údajů bylo

302 Obecné nařízení o ochraně osobních údajů, 39. bod odůvodnění.

přiměřené s ohledem na účel shromažďování a časově omezené, zejména v policejním sektoru.[303]

> Příklad: Ve věci *S. a Marper*[304] ESLP rozhodl, že neomezené uchovávání otisků prstů, vzorků buněk a profilů DNA dvou stěžovatelů nebylo přiměřené a nezbytné v demokratické společnosti, a to vzhledem k tomu, že trestněprávní řízení proti oběma stěžovatelům byla ukončena zproštěním viny v prvním případě a zpětvzetím obžaloby v případě druhém.

Časové omezení ukládání osobních údajů se vztahuje pouze na údaje uchovávané ve formě, která umožňuje identifikaci subjektů údajů. Zákonného ukládání údajů, které již nejsou zapotřebí, by proto mohlo být dosaženo anonymizací údajů.

Archivované údaje ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely mohou být uloženy po delší období, pokud tyto údaje budou využity výhradně pro výše uvedené účely.[305] Pro setrvalé ukládání a používání osobních údajů je nutné zavést vhodná technická a organizační opatření za účelem zabezpečení práv a svobod subjektu údajů.

Modernizovaná úmluva č. 108 rovněž umožňuje výjimky ze zásady omezení uložení pod podmínkou, že jsou stanoveny zákonem, respektují podstatu základních práv a svobod a jsou nezbytné a přiměřené ke sledování omezeného počtu legitimních cílů.[306] Mezi ně mimo jiné patří ochrana bezpečnosti státu, vyšetřování a stíhání trestných činů, výkon trestů, ochrana subjektu údajů a ochrana práv a základních svobod jiných osob.

303 Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04: viz také například: Rozsudek ESLP ze dne 13. listopadu 2012, *M. M. v. Spojené království*, č. 24029/07.

304 Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04.

305 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. e); Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b) a čl. 11 odst. 2.

306 Modernizovaná úmluva č. 108, čl. 11 odst. 1; Vysvětlující zpráva k Modernizované úmluvě č. 108, body 91–98.

Příklad: Ve věci *Digital Rights Ireland*[307] SDEU přezkoumával platnost směrnice o uchovávání údajů, jejímž cílem bylo harmonizovat vnitrostátní ustanovení pro uchovávání osobních údajů vytvářených nebo zpracovávaných veřejně dostupnými službami nebo sítěmi elektronických komunikací za účelem boje proti závažným trestným činům, jako je organizovaná trestná činnost a terorismus. Směrnice o uchovávání údajů stanoví uchovávání těchto údajů „po dobu nejméně šesti měsíců, aniž jakkoli rozlišuje mezi jednotlivými kategoriemi údajů uvedenými v článku 5 této směrnice podle jejich případné užitečnosti pro účely sledovaného cíle nebo podle dotčených osob".[308] SDEU rovněž upozornil na problém, že směrnice o uchovávání údajů neuvádí objektivní kritéria, na jejichž základě musí být určena přesná doba uchovávání údajů – jež se může pohybovat v rozmezí od nejméně šesti měsíců po nejvýše 24 měsíců – s cílem zajistit, že je tato doba omezena na nezbytné minimum.[309]

3.6. Zásada zabezpečení údajů

Hlavní body

- Zabezpečení a důvěrnost osobních údajů jsou stěžejní pro to, aby se zabránilo nepříznivým dopadům na subjekt údajů.
- Bezpečnostní opatření mohou být technické a/nebo organizační povahy.
- Jedním z procesů, který může ochránit osobní údaje, je pseudonymizace.
- Vhodnost bezpečnostních opatření musí být stanovena v každém jednotlivém případě a pravidelně přezkoumávána.

Zásada bezpečnosti údajů vyžaduje, aby při zpracování osobních údajů byla provedena vhodná technická nebo organizační opatření s cílem chránit údaje před náhodným, neoprávněným nebo protiprávním přístupem, použitím, změnou, zpřístupněním, ztrátou, zničením nebo poškozením. [310] GDPR stanoví, že správce

307 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

308 Tamtéž, bod 63.

309 Tamtéž, bod 64.

310 Obecné nařízení o ochraně osobních údajů, 39. bod odůvodnění a čl. 5 odst. 1 písm. f); Modernizovaná úmluva č. 108, článek 7.

a zpracovatel by měli při provádění těchto opatření přihlédnout „ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob“.[311] V závislosti na zvláštních okolnostech daného případu by k vhodným technickým a organizačním opatřením mohla patřit například pseudonymizace a šifrování osobních údajů a/nebo pravidelné testování a hodnocení účinnosti příslušných opatření s cílem zajistit zabezpečení zpracování údajů.[312]

Jak bylo vysvětleno v oddíle 2.1.1, pseudonymizace údajů znamená nahrazení prostředků přiřazování v osobních údajích – což znemožní identifikaci subjektu údajů – pseudonymem a samostatné vedení těchto prostředků přiřazování za pomoci technických či organizačních opatření. Proces pseudonymizace nesmí být zaměňován s procesem anonymizace, kdy jsou odstraněna veškerá vodítka k identifikaci dané osoby.

Příklad: Větu „Charles Spencer, narozen dne 3. dubna 1967, je otcem rodiny se čtyřmi dětmi, dvěma chlapci a dvěma děvčaty“ lze například pseudonymizovat takto:

„C. S. 1967 je otec rodiny se čtyřmi dětmi, dvěma chlapci a dvěma děvčaty“ nebo

„324 je otec rodiny se čtyřmi dětmi, dvěma chlapci a dvěma děvčaty“ nebo

„YESz3201 je otec rodiny se čtyřmi dětmi, dvěma chlapci a dvěma děvčaty“.

Uživatelé, kteří mají přístup ke pseudonymizovaným údajům, obvykle nebudou moci identifikovat „Charlese Spencera, narozeného dne 3. dubna 1967“ pomocí kódu „324“ nebo „YESz3201“. Je tudíž pravděpodobnější, že budou tyto údaje zabezpečeny před zneužitím.

První příklad je však méně zabezpečený. Pokud je věta „C. S. 1967 je otec rodiny se čtyřmi dětmi, dvěma chlapci a dvěma děvčaty“ použita v malé vesnici, kde Charles Spencer žije, může být pan Spencer snadno rozpoznatelný. Metoda pseudonymizace může ovlivnit účinnost ochrany údajů.

311 Obecné nařízení o ochraně osobních údajů, čl. 32 odst. 1.

312 Tamtéž.

Osobní údaje se zašifrovanými nebo samostatně uchovávanými prostředky přiřazování se používají v řadě různých souvislostí jako prostředek, jak uchovávat osobní identity v tajnosti. To je zvlášť užitečné, pokud správci údajů musejí zajistit, že jde o tentýž subjekt údajů, ale není nutné znát skutečnou identitu subjektů údajů a ani tato znalost není žádoucí. Tak je tomu například v případě, kdy výzkumný pracovník studuje průběh nemoci u pacientů, jejichž identita je známa pouze nemocnici, kde byli léčeni a od níž výzkumný pracovník získává pseudonymizovanou anamnézu. Pseudonymizace je tudíž účinný prostředek, který mají technologie na posílení soukromí k dispozici. Může fungovat jako významný prvek při zavádění standardní ochrany soukromí. To znamená, že ochrana údajů je zabudována již do samotných základů systémů ochrany údajů.

Článek 25 nařízení GDPR, který se zabývá záměrnou ochranou údajů, výslovně odkazuje na pseudonymizaci jako na příklad vhodného technického a organizačního opatření, které by měli správci zavést, aby vyhověli zásadám ochrany údajů a začlenili nezbytné záruky. Tím správci vyhoví požadavkům tohoto nařízení a budou chránit práva subjektů údajů při zpracování jejich osobních údajů.

Soulad s požadavky na bezpečnost zpracování může pomoci doložit dodržování schváleného kodexu chování nebo schváleného mechanismu pro vydávání osvědčení.[313] Rada Evropy ve svém stanovisku k důsledkům zpracovávání jmenné evidence cestujících pro ochranu údajů uvádí další příklady vhodných bezpečnostních opatření na ochranu osobních údajů v systémech jmenné evidence cestujících. K těmto požadavků patří uchovávání údajů v zabezpečeném fyzickém prostředí s řízením omezeného přístupu pomocí přihlašovacích údajů a chránícím sdělování údajů silnými kryptografickými opatřeními.[314]

Příklad: Stránky sociálních sítí a poskytovatelé e-mailových služeb umožňují uživatelům přidat další úroveň zabezpečení údajů u služeb, které poskytují, prostřednictvím zavedení dvoustupňového ověřování. Kromě zadání osobního hesla musí uživatelé provést druhé přihlášení, aby získali přístup ke svému osobnímu účtu. Toto druhé přihlášení může mít například podobu zadání bezpečnostního kódu zaslaného na číslo mobilního telefonu

313 Tamtéž, čl. 32 odst. 3.

314 Rada Evropy, Výbor zřízený podle Úmluvy č. 108, *Opinion on the Data protection implications of the processing of Passenger Name Records* [Stanovisko k důsledkům zpracovávání jmenné evidence cestujících pro ochranu údajů], T-PD(2016)18rev, 19. srpna 2016, s. 9.

připojeného k osobnímu účtu. Tím poskytuje dvoustupňové ověření lepší ochranu osobních informací před neoprávněným přístupem k osobnímu účtu prostřednictvím hackingu.

Vysvětlující zpráva k Modernizované úmluvě č. 108 uvádí další příklady vhodných záruk, jako je zavedení povinnosti zachovávat služební tajemství nebo přijetí kvalifikovaných opatření v oblasti technického zabezpečení, např. šifrování údajů.[315] Při zavádění zvláštních bezpečnostních opatření by správce – nebo případně zpracovatel – měl zohlednit několik prvků, například povahu a objem zpracovávaných osobních údajů, případné nepříznivé dopady na subjekty údajů a nutnost omezení přístupu k údajům.[316] Při provádění vhodných bezpečnostních opatření je třeba zvážit současné špičkové metody a techniky zabezpečení údajů za účelem jejich zpracovávání. Náklady na tato opatření musí být přiměřené závažnosti a pravděpodobnosti možných rizik. Je zapotřebí provádět pravidelný přezkum bezpečnostních opatření, aby mohla být podle potřeby aktualizována.[317]

V případech, kdy dojde k porušení zabezpečení osobních údajů, ukládá Modernizovaná úmluva č. 108 i GDPR správci povinnost neprodleně oznámit porušení příslušnému dozorovému úřadu spolu s riziky, jež z toho vyplývají pro práva a svobody jednotlivců.[318] V případě, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva nebo svobody subjektu údajů, existuje podobná povinnost oznámit událost tomuto subjektu.[319] Oznámení o porušení zabezpečení údajů určené subjektu údajů musí používat jasné a jednoduché jazykové prostředky.[320] Pokud se zpracovatel dozví o porušení zabezpečení osobních údajů, musí tuto skutečnost neprodleně oznámit správci.[321] V některých situacích mohou platit výjimky z oznamovací povinnosti. Například není nutné, aby správce informoval dozorový úřad, pokud „ je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob".[322] Také není nutné informovat subjekt údajů, pokud zavedená bezpečnostní opatření činí tyto údaje nesrozumitelnými pro osoby, které nejsou oprávněny k nim mít přístup, nebo když následná opatření zajistí, že se

315 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 56.

316 Tamtéž, bod 62.

317 Tamtéž, bod 63.

318 Modernizovaná úmluva č. 108, čl. 7 odst. 2; obecné nařízení o ochraně osobních údajů, čl. 33 odst. 1.

319 Modernizovaná úmluva č. 108, čl. 7 odst. 2; obecné nařízení o ochraně osobních údajů, čl. 34 odst. 1.

320 Obecné nařízení o ochraně osobních údajů, čl. 34 odst. 2.

321 Tamtéž, čl. 33 odst. 1.

322 Tamtéž, čl. 32 odst. 1.

vysoké riziko již pravděpodobně neprojeví.[323] Pokud by sdělení o porušení zabezpečení osobních údajů subjektu údajů vyžadovala nepřiměřené úsilí ze strany správce, může povinnost, aby byly „subjekty údajů informovány stejně účinným způsobem", zajistit veřejné oznámení nebo podobné opatření.[324]

3.7. Zásada odpovědnosti

Hlavní body

- Podle zásady odpovědnosti musí správci a zpracovatelé při svých zpracovatelských činnostech aktivně a průběžně provádět opatření na podporu a zaručení ochrany údajů.
- Správci a zpracovatelé nesou odpovědnost za to, že jejich operace zpracovávání budou v souladu s právem v oblasti ochrany údajů a s jejich příslušnými povinnostmi.
- Správci musí být schopni kdykoliv doložit subjektům údajů, široké veřejnosti a dozorovým úřadům, že jednají v souladu s ustanoveními na ochranu údajů. Zpracovatelé také musí plnit určité povinnosti, které jsou důsledně spojeny s odpovědností (například vedení záznamů o operacích zpracovávání a jmenování pověřence pro ochranu osobních údajů).

GDPR a Modernizovaná úmluva č. 108 stanoví, že správce nese zodpovědnost za dodržování zásad zpracování osobních údajů popsaných v této kapitole a musí být schopen toto dodržování doložit.[325] Za tímto účelem musí správce zavést vhodná technická a organizační opatření.[326] I když zásada odpovědnosti směřuje v čl. 5 odst. 2 GDPR pouze proti správcům, i od zpracovatelů se očekává, že ponesou odpovědnost, jelikož musejí plnit několik povinností a jejich úloha úzce souvisí s odpovědností.

Právní předpisy EU a RE v oblasti ochrany údajů rovněž stanoví, že správce je odpovědný za dodržování zásad ochrany údajů pojednaných v oddílech 3.1 až 3.6 a měl by být schopen toto dodržování zajistit.[327] Pracovní skupina zřízená podle článku 29

323 Tamtéž, čl. 34 odst. 3 písm. a) a b).

324 Tamtéž, čl. 34 odst. 3 písm. c).

325 Tamtéž, čl. 5 odst. 2; Modernizovaná úmluva č. 108, čl. 10 odst. 1.

326 Obecné nařízení o ochraně osobních údajů, článek 24.

327 Tamtéž, čl. 5 odst. 2; Modernizovaná úmluva č. 108, čl. 10 odst. 1.

poukazuje na to, že „druhy postupů a mechanismů se budou lišit podle rizik vyplývajících ze zpracování a povahy údajů“.[328]

Správci mohou různými způsoby usnadnit dodržování tohoto požadavku, a to kromě jiného:

- vedením záznamů o činnostech zpracování a jejich poskytnutím na požádání dozorovému úřadu,[329]
- v některých případech jmenováním pověřence pro ochranu osobních údajů, který je zapojen do všech otázek souvisejících s ochranou osobních údajů,[330]
- provedením posouzení vlivu na ochranu údajů v případě těch druhů zpracování, které by pravděpodobně měly za následek vysoké riziko pro práva a svobody fyzických osob,[331]
- zajištěním záměrné a standardní ochrany osobních údajů,[332]
- zavedením postupů pro výkon práv subjektů údajů,[333]
- dodržováním schválených kodexů chování nebo schválených mechanismů pro vydávání osvědčení.[334]

Ačkoliv zásada odpovědnosti v čl. 5 odst. 2 GDPR není výslovně cílena na zpracovatele, existují ustanovení spojená s odpovědností, která obsahují také povinnosti pro zpracovatele, například vedení záznamů o činnostech zpracování a jmenování pověřence pro ochranu osobních údajů pro veškeré činnosti zpracování, pro které je pověřenec zapotřebí.[335] Zpracovatelé musí také zajistit, že byla provedena veškerá opatření nezbytná k zajištění zabezpečení údajů.[336] Právně závazná smlouva mezi správcem a zpracovatelem musí stanovit, že zpracovatel bude správci nápomocen

328 Pracovní skupina zřízená podle článku 29, *Stanovisko č. 3/2010 k zásadě odpovědnosti*, WP 173, Brusel, 13. července 2010, bod 12.

329 Obecné nařízení o ochraně osobních údajů, článek 30.

330 Tamtéž, články 37–39.

331 Tamtéž, článek 35; Modernizovaná úmluva č. 108, čl. 10 odst. 2.

332 Obecné nařízení o ochraně osobních údajů, článek 25; Modernizovaná úmluva č. 108, čl. 10 odst. 2 a 3.

333 Tamtéž, článek 12 a článek 24.

334 Tamtéž, článek 40 a článek 42.

335 Tamtéž, čl. 5 odst. 2, články 30 a 37.

336 Tamtéž, čl. 28 odst. 3 písm. c).

při plnění některých požadavků stanovených právními předpisy, například při provádění posouzení vlivu na ochranu osobních údajů nebo povinnost oznámit správci jakékoliv porušení zabezpečení ochrany osobních údajů, jakmile se o něm dozví.[337]

Organizace pro hospodářskou spolupráci a rozvoj (OECD) přijala v roce 2013 pokyny týkající soukromí, v nichž se zdůrazňuje, že správci plní důležitou úlohu při zajišťování funkčnosti ochrany údajů v praxi. Pokyny pojednávají o zásadě odpovědnosti v tom smyslu, že „správce údajů by měl být odpovědný za soulad s opatřeními, která provádějí tyto [materiální] zásady uvedené výše".[338]

Příklad: Legislativním příkladem zdůrazňujícím zásadu odpovědnosti je změna[339] směrnice 2002/58/ES o soukromí a elektronických komunikacích z roku 2009. Podle článku 4 v pozměněném znění ukládá směrnice povinnost „zajistit provádění bezpečnostní politiky týkající se zpracování osobních údajů". Normotvůrce tudíž, pokud jde o bezpečnostní ustanovení uvedené směrnice, rozhodl, že je nezbytné zavést výslovný požadavek na to mít a provádět bezpečnostní politiku.

Podle stanoviska pracovní skupiny zřízené podle článku 29[340] je podstatou odpovědnosti povinnost správce činit následující kroky:

- mít zavedená opatření, která by – za běžných podmínek – zaručila, že budou dodržována pravidla ochrany údajů v souvislosti s operacemi zpracování, a

- mít připravenou dokumentaci, která subjektům údajů a dozorovým úřadům dokládá, že byla přijata opatření k dosažení souladu s pravidly v oblasti ochrany údajů.

Zásada odpovědnosti tudíž vyžaduje, aby správci aktivně doložili soulad a nečekali jen na to, až subjekty údajů nebo dozorové orgány poukáží na nedostatky.

337 Tamtéž, čl. 28 odst. 3 písm. d).

338 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data [Pokyny upravující ochranu soukromí a přeshraniční toky osobních údajů]*, článek 14.

339 Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, Úř. věst. 2009 L 337, s. 11.

340 Pracovní skupina zřízená podle článku 29, *Stanovisko č. 3/2010 k zásadě odpovědnosti*, WP 173, Brusel, 13. července 2010.

4

Pravidla evropského práva v oblasti ochrany údajů

EU	Pojednávaná témata	RE
Pravidla týkající se zákonného zpracování údajů		
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. a) Rozsudek SDEU z roku 2011, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland* Rozsudek SDEU z roku 2017, C-536/15, *Tele2 (Netherlands) BV a další v. Autoriteit Consument en Markt (AMC)*	**Souhlas**	Doporučení o profilování, čl. 3.4 písm. b) a článek 3.6 Modernizovaná úmluva č. 108, čl. 5 odst. 2
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. b)	**(Před)smluvní vztah**	Doporučení o profilování, čl. 3.4 písm. b)
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. c)	**Právní povinnosti správce**	Doporučení o profilování, čl. 3.4 písm. a)
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. d)	**Životně důležité zájmy subjektu údajů**	Doporučení o profilování, čl. 3.4 písm. b)
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. e) Rozsudek SDEU (velkého senátu) z roku 2008, C-524/06, *Huber v. Bundesrepublik Deutschland*	**Veřejný zájem a výkon veřejné moci**	Doporučení o profilování, čl. 3.4 písm. b)

EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. f) Rozsudek SDEU z roku 2017, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme“* Rozsudek SDEU z roku 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*	**Oprávněné zájmy dalších osob**	Doporučení o profilování, čl. 3.4 písm. b) Rozsudek ESLP z roku 2015, *Y. v. Turecko*, č. 648/10
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 4	**Výjimka z účelového omezení: další zpracování pro jiné účely**	Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b)
Pravidla týkající se zákonného zpracování citlivých osobních údajů		
Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 1	**Obecný zákaz zpracování**	Modernizovaná úmluva č. 108, článek 6
Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2	**Výjimky z obecného zákazu**	Modernizovaná úmluva č. 108, článek 6
Pravidla zabezpečeného zpracování		
Obecné nařízení o ochraně osobních údajů, článek 32	**Povinnost zajistit zabezpečené zpracování**	Modernizovaná úmluva č. 108, čl. 7 odst. 1 Rozsudek ESLP z roku 2008, *I. v. Finsko*, č. 20511/03
Obecné nařízení o ochraně osobních údajů, článek 28 a čl. 32 odst. 1 písm. b)	**Povinnost mlčenlivosti**	Modernizovaná úmluva č. 108, čl. 7 odst. 1
Obecné nařízení o ochraně osobních údajů, článek 34 Směrnice o soukromí a elektronických komunikacích, čl. 4 odst. 2	**Ohlášení případů porušení zabezpečení osobních údajů**	Modernizovaná úmluva č. 108, čl. 7 odst. 2
Pravidla odpovědnosti a prosazování souladu s právními předpisy		
Obecné nařízení o ochraně osobních údajů, článek 12, 13 a 14	**Transparentnost obecně**	Modernizovaná úmluva č. 108, článek 8
Obecné nařízení o ochraně osobních údajů, článek 37, 38 a 39	**Pověřenci pro ochranu osobních údajů**	Modernizovaná úmluva č. 108, čl. 10 odst. 1

EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů, článek 30	**Záznamy o činnostech zpracování**	
Obecné nařízení o ochraně osobních údajů, článek 35 a 36	**Posouzení vlivu a předchozí konzultace**	Modernizovaná úmluva č. 108, čl. 10 odst. 2
Obecné nařízení o ochraně osobních údajů, článek 33 a 34	**Ohlášení případů porušení zabezpečení osobních údajů**	Modernizovaná úmluva č. 108, čl. 7 odst. 2
Obecné nařízení o ochraně osobních údajů, článek 40 a 41	**Kodexy chování**	
Obecné nařízení o ochraně osobních údajů, článek 42 a 43	**Vydávání osvědčení**	
Záměrná a standardní ochrana osobních údajů		
Obecné nařízení o ochraně osobních údajů, čl. 25 odst. 1 písm. a)	**Záměrná ochrana osobních údajů**	Modernizovaná úmluva č. 108, čl. 10 odst. 2
Obecné nařízení o ochraně osobních údajů, čl. 25 odst. 1 písm. b)	**Standardní ochrana osobních údajů**	Modernizovaná úmluva č. 108, čl. 10 odst. 3

Zásady nutně musejí být obecné povahy. Jejich uplatnění v konkrétních situacích ponechává určitý prostor pro vlastní uvážení, pokud jde o výklad a výběr prostředků. Podle **práva RE** záleží na smluvních stranách Modernizované úmluvy č. 108, zda vyjasní tento prostor pro vlastní výklad ve svém vnitrostátním právním řádu. Pokud jde o **právo EU**, je situace odlišná: pro účely zajištění ochrany údajů na vnitřním trhu bylo uznáno za nezbytné mít podrobnější pravidla na úrovni EU s cílem harmonizovat úroveň ochrany údajů vnitrostátních právních předpisů členských států. Obecné nařízení o ochraně osobních údajů stanoví vrstvu podrobných pravidel podle zásad stanovených v článku 5, které jsou přímo použitelné ve vnitrostátním právní řádu. Níže uvedené poznámky k podrobným pravidlům ochrany údajů na evropské úrovni se proto zabývají převážně právem EU.

4.1. Pravidla týkající se zákonného zpracování

Hlavní body

- Osobní údaje mohou být zákonně zpracovávány, pokud splňují jedno z níže uvedených kritérií:
  - zpracování je založeno na souhlasu subjektu údajů,
  - smluvní vztah vyžaduje zpracování osobních údajů,
  - zpracování je nutné za účelem dodržování právních povinností správce,
  - životně důležité zájmy subjektů údajů nebo jiné osoby vyžadují zpracovávání jejich údajů,
  - zpracování je nezbytné pro splnění úkolu ve veřejném zájmu,
  - oprávněné zájmy správců nebo třetích stran jsou důvodem pro zpracování, ale pouze pokud nejsou převáženy zájmy nebo základními právy subjektů údajů.
- Zákonné zpracovávání citlivých osobních údajů podléhá zvláštnímu, přísnějšímu režimu.

4.1.1. Zákonné důvody pro zpracování údajů

Kapitola II GDPR s názvem „Zásady" stanoví, že zpracování veškerých osobních údajů musí být v souladu především se zásadami souvisejícími s kvalitou údajů, stanovenými v článku 5 obecného nařízení o ochraně osobních údajů. Jednou z těchto zásad je, že by osobní údaje měly být „zpracovávány korektně a zákonným a transparentním způsobem". Zadruhé, aby údaje byly zpracovány zákonným způsobem, musí být zpracování v souladu s jedním ze zákonných důvodů pro oprávněné zpracování údajů uvedených v článku 6[341] v případě jiných než citlivých osobních údajů a v článku 9 v případě zvláštních kategorií údajů (neboli citlivých údajů). Obdobně kapitola II Modernizované úmluvy č. 108, která určuje „základní zásady pro ochranu

341 Rozsudek SDEU ze dne 20. května 2003, spojené věci C-465/00, C-138/01 a C-139/01, *Rechnungshof v. Österreichischer Rundfunk a další a Christa Neukomm a Jospeh Lauermann v. Österreichischer Rundfunk*, bod 65; rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, bod 48; rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, bod 26.

údajů“, stanoví, že má-li být zpracování údajů zákonné, musí být „přiměřené ve vztahu ke sledovanému oprávněnému účelu“.

Bez ohledu na zákonné důvody zpracování, o které se správce opírá při zahájení operací zpracování osobních údajů, bude správce také muset uplatnit záruky stanovené v režimu obecného práva na ochranu údajů.

Souhlas

V rámci práva RE je souhlas uveden v čl. 5 odst. 2 Modernizované úmluvy č. 108. Rovněž na něj odkazuje judikatura ESLP a několik doporučení RE.[342] **Podle práva EU** je souhlas jako základ pro zákonné zpracování údajů pevně stanoven v článku 6 GDPR a je také výslovně uveden v článku 8 Listiny. Charakteristiky platného souhlasu jsou vysvětleny v definici souhlasu uvedené v článku 4, zatímco podmínky pro získání platného souhlasu jsou podrobně uvedeny v článku 7 a zvláštní pravidla pro souhlas dítěte v souvislosti se službami informační společnosti jsou stanoveny v článku 8 GDPR.

Jak je vysvětleno v oddíle 2.4, souhlas musí být svobodný, konkrétní, informovaný a jednoznačný. Souhlas musí být prohlášením či zjevným potvrzením svolení ke zpracování a daná osoba má právo svůj souhlas kdykoli odvolat. Správci mají povinnost uchovávat ověřitelný záznam o souhlasu.

Svobodný souhlas

V právním systému **RE** podle Modernizované úmluvy č. 108 musí souhlas subjektu údajů „představovat svobodné vyjádření úmyslného rozhodnutí“.[343] Svobodný souhlas je platný jen tehdy, „když má subjekt údajů skutečnou možnost volby a neexistuje žádné riziko klamání, zastrašování, nátlaku či podstatných záporných důsledků, jestliže souhlas neudělí“.[344] V této souvislosti **právo EU** stanoví, že souhlas není považován za svobodný, „pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen“.[345] V GDPR se

342 Viz například Rada Evropy, Výbor ministrů (2010): Doporučení CM/Rec(2010)13 Výboru ministrů členským státům o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů v kontextu profilování, 23. listopadu 2010, čl. 3.4 písm. b).

343 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 42.

344 Viz pracovní skupina zřízená podle článku 29 (2011), *Stanovisko č. 15/2011 k definici souhlasu*, WP 187, Brusel, 13. července 2011, s. 12.

345 Obecné nařízení o ochraně osobních údajů, 42. bod odůvodnění.

zdůrazňuje, že „[p]ři posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné".[346] Vysvětlující zpráva k Modernizované úmluvě č. 108 uvádí, že „[n]esmí docházet k žádnému nekalému ovlivňování subjektu údajů nebo nátlaku na něj (který může být hospodářské nebo jiné povahy), ať už přímému, nebo nepřímému, a souhlas by neměl být považován za svobodný, pokud nemá subjekt údajů skutečnou volbu nebo nemůže odmítnout nebo vzít zpět svůj souhlas, aniž by mu hrozila újma".[347]

Příklad: Některé obce ve státě A se rozhodly, že zřídí pobytovou kartu se zabudovaným čipem. Pro rezidenty není získání této elektronické karty povinné. Avšak rezidenti, kteří kartu nevlastní, nemají přístup k řadě důležitých správních služeb, např. možnost platit obecní daně on-line, předkládat stížnosti elektronickou cestou a využívat třídenní lhůty, do které musí orgány odpovědět, a dokonce vyhnout se frontám, nakupovat zlevněné lístky při návštěvě obecní koncertní síně a používat skenery u vchodu.

Zpracování osobních údajů ze strany obcí v tomto případě nemůže být založeno na souhlasu. Jelikož se zde na rezidenty vyvíjí přinejmenším nepřímý tlak na získání elektronické karty a udělení souhlasu se zpracováním, není souhlas svobodný. Vývoj systému elektronických karet ze strany obcí by tudíž měl být založen na jiném legitimním důvodu odůvodňujícím zpracování. Například by se mohli odvolávat na to, že zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, což je zákonný základ pro zpracování podle čl. 6 odst. 1 písm. e) GDPR.[348]

Svobodný souhlas by byl sporný také v situaci podřízenosti, kdy existuje významná hospodářská nebo jiná nerovnováha mezi správcem, který získává souhlas,

346 Tamtéž, čl. 7 odst. 4.

347 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 42.

348 Pracovní skupina zřízená podle článku 29 (2011), *Stanovisko č. 15/2011 k definici souhlasu*, WP 187, Brusel, 13. července 2011, s. 16. Další příklady případů, kdy zpracování údajů nemůže být založeno na souhlasu, ale vyžaduje jiný právní základ pro legitimizaci zpracování, lze nalézt na s. 14 a 17 uvedeného stanoviska.

a subjektem údajů, který souhlas poskytuje.[349] Typickým příkladem těchto nerovnováh a podřízenosti je zpracování osobních údajů prováděné zaměstnavatelem v souvislosti se zaměstnaneckým vztahem. Podle pracovní skupiny zřízené podle článku 29 „[z]aměstnanci nejsou téměř nikdy v postavení, aby mohli dát souhlas svobodně nebo ho odmítnout či odvolat, což je dáno závislostí vyplývající ze vztahu zaměstnavatel/zaměstnanec. Vzhledem k nerovnováze sil mohou zaměstnanci udělit svobodný souhlas jen za výjimečných okolností, kdy souhlas nebo odmítnutí nevyvolá žádné následky."[350]

Příklad: Jistá velká společnost plánuje vytvořit adresář obsahující jména všech zaměstnanců, jejich funkce ve společnosti a jejich pracovní adresy, a to výlučně za účelem zlepšení vnitřní komunikace ve společnosti. Personální vedoucí navrhuje přidat do adresáře fotografii každého zaměstnance, aby bylo možné kolegy na schůzích snáze rozeznat. Zástupci zaměstnanců trvají na to, že by fotografie měly být doplněny, pouze pokud k tomu dotyční zaměstnanci udělí souhlas.

V takové situaci by měl být souhlas zaměstnance uznán jako právní základ pro zpracování fotografií v adresáři, protože je věrohodné, že zaměstnanec nepocítí vůbec žádné důsledky, ať už se rozhodne souhlas se zveřejněním své fotografie v adresáři udělit, či nikoliv.

Příklad: Společnost A plánuje schůzi tří svých zaměstnanců s řediteli společnosti B za účelem projednání případné budoucí spolupráce na určitém projektu. Schůze se bude konat v prostorách společnosti B, která po společnosti A požaduje, aby jí zaslala e-mailem jména, životopisy a fotografie účastníků této schůze. Společnost B argumentuje tím, že potřebuje jména a fotografie účastníků k tomu, aby pracovníci ochranky u vchodu do budovy mohli ověřit, že jde o správné osoby, a životopisy pak ředitelům umožní se na schůzi lépe připravit. V tomto případě předání osobních údajů zaměstnanců ze strany společnosti A nelze založit na souhlasu. Souhlas nelze považovat za „svobodný", protože je možné, že zaměstnanci mohou čelit negativním

349 Viz také pracovní skupina zřízená podle článku 29 (2001), *Stanovisko 8/2001 o zpracování osobních údajů v souvislosti se zaměstnáním*, WP 48, Brusel, 13. září 2001; pracovní skupina zřízená podle článku 29 (2005), Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995, WP 114, Brusel, 25. listopadu 2005; pracovní skupina zřízená podle článku 29 (2017), *Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti*, WP 249, Brusel, 8. června 2017.

350 Pracovní skupina zřízená podle článku 29, *Stanovisko 2/2017 ke zpracování údajů na pracovišti*, WP 249, Brusel, 8. června 2017.

důsledkům, pokud nabídku odmítnou (například mohou být nahrazeni jiným kolegou, a to nejen pokud jde o účast na schůzi, ale také ve vyjednávání se společností B a obecně v práci na tomto projektu). Proto musí být zpracování založeno na jiném zákonném důvodu pro zpracování.

To však neznamená, že souhlas nemůže být nikdy platný za okolností, kdy by neudělení souhlasu mělo negativní důsledky. Například pokud situace, kdy zákazník neudělí souhlas s vlastnictvím zákaznické karty jistého supermarketu, bude mít za následek pouze to, že nezíská malou slevu z ceny určitého zboží, mohl by souhlas být platným právním základem pro zpracování osobních údajů těch zákazníků, kteří souhlasili s vlastnictvím takovéto karty. Mezi společností a zákazníkem neexistuje podřízenost a důsledky neudělení souhlasu nejsou dostatečně závažné, aby zabránily subjektu údajů v tom, aby přijal svobodné rozhodnutí (pokud je snížení ceny dostatečně nízké, aby neovlivnilo jejich svobodné rozhodování).

Pokud však lze zboží a služby získat pouze pod podmínkou sdělení určitých osobních údajů správci nebo dále třetím stranám, souhlas subjektů údajů se zveřejněním svých údajů, které nejsou pro danou smlouvu nezbytné, nelze považovat za svobodné rozhodnutí, a není proto platný podle práva v oblasti ochrany údajů.[351] GDPR poměrně důrazně zakazuje podmiňovat poskytnutí výrobků a služeb udělením souhlasu.[352]

Příklad: Souhlas cestujících s tím, že letecký dopravce předá takzvanou jmennou evidenci cestujících (tj. údaje o jejich totožnosti, stravovacích návycích nebo zdravotních potížích) imigračním orgánům dané cizí země, nelze považovat za platný souhlas podle práva v oblasti ochrany údajů, protože cestující nemají na výběr, pokud chtějí navštívit danou zemi. Mají-li být tyto údaje předány zákonně, je nutný jiný právní základ než souhlas, nejpravděpodobněji zvláštní právní předpis.

Informovaný souhlas

Subjekt údajů musí mít předtím, než se rozhodne, dostatečné informace. Informovaný souhlas obvykle sestává z přesného a snadno srozumitelného popisu dané věci vyžadující souhlas. Jak vysvětluje pracovní skupina zřízená podle článku 29, souhlas musí být založen na uvědomění si a pochopení skutečností a důsledků toho,

351 Obecné nařízení o ochraně osobních údajů, čl. 7 odst. 4.

352 Tamtéž.

že subjekt údajů udělí souhlas se zpracováním. Proto „[d]otčené osobě musejí být jasným a srozumitelným způsobem poskytnuty přesné a úplné informace o všech podstatných otázkách […], jako jsou povaha zpracovávaných údajů, účely zpracování, příjemci, jimž budou údaje případně předány, a práva subjektu údajů".[353] Aby byl souhlas informovaný, musejí si jednotlivci být také vědomi důsledků toho, když neudělí souhlas se zpracováním.

Vzhledem k významu informovaného souhlasu usilovaly GDPR a Vysvětlující zpráva k Modernizované úmluvě č. 108 o objasnění tohoto pojmu. Body odůvodnění GDPR stanoví, že informovaný souhlas znamená, že by měl „subjekt údajů znát alespoň totožnost správce a účely zpracování, k nimž jsou" jeho zpracovávané osobní údaje určeny.[354]

Ve výjimečném případě souhlasu použitého jako odchylka za účelem zajištění zákonného důvodu pro mezinárodní předání údajů musí správce informovat subjekt údajů o možných rizicích předání, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, má-li být souhlas považován za platný.[355]

Vysvětlující zpráva k Modernizované úmluvě č. 108 upřesňuje, že je nutné poskytnout informace o důsledcích rozhodnutí subjektu údajů, konkrétně „co skutečnost udělení souhlasu obnáší a rozsah, v jakém je souhlas udílí".[356]

Je důležitá kvalita informací. Kvalitou informací se rozumí, že by jazykové prostředky, jimiž se tyto informace sdělují, měly být uzpůsobeny očekávaným příjemcům. Informace musí být podány bez žargonu, srozumitelným a jednoduchým jazykem, kterému by měl rozumět běžný uživatel.[357] Informace musí být také snadno dostupné subjektu údajů a mohou být poskytnuty ústně nebo písemně. Důležitými prvky jsou přístupnost a viditelnost informací: informace musí být jasně viditelné a výrazné. V on-line prostředí mohou být dobrým řešením několikavrstvá upozornění, protože umožňují subjektům údajů rozhodnout se, zda si přečtou stručné nebo podrobnější znění informací.

353 Pracovní skupina zřízená podle článku 29 (2007), Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR), WP 131, Brusel, 15. února 2007.

354 Obecné nařízení o ochraně osobních údajů, 42. bod odůvodnění.

355 Tamtéž, čl. 49 odst. 1 písm. a).

356 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 42.

357 Pracovní skupina zřízená podle článku 29 (2011), *Stanovisko č. 15/2011 k definici souhlasu*, WP 187, Brusel, 13. července 2011, s. 19.

Konkrétní souhlas

Má-li být souhlas platný, musí být také určen konkrétně pro daný účel zpracování, který musí být jasně a jednoznačně popsán. To je slučitelné s kvalitou informací poskytnutých o účelu udělení souhlasu. V této souvislosti budou důležitá přiměřená očekávání průměrného subjektu údajů. Subjekt údajů musí být požádán o nový souhlas, pokud mají být přidány nebo změněny operace zpracování způsobem, který nebylo možné rozumně předvídat, když byl udělen původní souhlas, a tudíž může dojít ke změně účelu. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny.[358]

Příklady: Ve věci *Deutsche Telekom AG*[359] SDEU zvažoval, zda poskytovatel telekomunikačních služeb, který musel předat osobní údaje účastníků za účelem zveřejnění v účastnických seznamech, potřeboval nový souhlas subjektů údajů[360], protože příjemci údajů nebyli původně uvedeni v době udělení souhlasu.

SDEU rozhodl, že podle článku 12 směrnice o soukromí a elektronických komunikacích nebylo získání nového souhlasu před předáním údajů nezbytné. Jelikož subjekty údajů měly pouze možnost souhlasit s účelem zpracování – jímž je zveřejnění jejich údajů –, nemohly si vybrat mezi různými seznamy, v nichž by tyto údaje mohly být zveřejněny.

Jak SDEU zdůraznil: „z kontextuálního a systematického výkladu článku 12 směrnice „o soukromí a elektronických komunikacích" vyplývá, že souhlas podle druhého odstavce tohoto článku se váže k účelu zveřejnění osobních údajů ve veřejně přístupném účastnickém seznamu, a nikoli k totožnosti konkrétního poskytovatele tohoto seznamu."[361] Kromě toho „samotné zveřejnění osobních údajů v účastnickém seznamu majícím zvláštní účel může účastníka poškodit"[362], a nejde tu tedy v první řadě o totožnost poskytovatele.

358 Obecné nařízení o ochraně osobních údajů, 32. bod odůvodnění.

359 Rozsudek SDEU ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*. Viz zejména body 53 a 54.

360 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. červenec 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, Úř. věst. 2002 L 201 (směrnice o soukromí a elektronických komunikacích).

361 Rozsudek SDEU ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, bod 61.

362 Tamtéž, bod 62.

Věc *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV v. Autoriteit Consument en Markt (AMC)*[363] se týkala žádosti belgické společnosti o to, aby jí informační služba o účastnických číslech a poskytování účastnických seznamů společnostem, které přidělují telefonní čísla v Nizozemsku, poskytla přístup k údajům týkajícím se účastníků. Belgická společnost se opírala o závazek podle směrnice o univerzální službě.[364] Ta společnostem ukládá, aby přiřazovaly telefonní čísla tak, aby je učinily přístupnými pro účastnické seznamy, které o tato čísla požádají, pokud účastníci udělí souhlas se zveřejněním svých čísel. Nizozemské společnosti toto odmítly s odvoláním na to, že nejsou povinné poskytovat dotčené údaje podniku usazenému v jiném členském státě. Namítaly, že uživatelé jim dali souhlas se zveřejněním svých čísel, protože se domnívali, že čísla budou zveřejněna v nizozemském účastnickém seznamu. SDEU rozhodl, že směrnice o univerzální službě zahrnuje veškeré žádosti podané podniky informačních služeb, bez ohledu na členský stát, v němž jsou podniky usazeny. SDEU také rozhodl, že poskytnutím těchto údajů jinému podniku za účelem jejich zveřejnění ve veřejně dostupném účastnickém seznamu tohoto podniku bez opětovného souhlasu uděleného tímto účastníkem není ohrožena samotná podstata práva na ochranu osobních údajů.[365] Není tedy nutné, aby podnik, který přiděluje telefonní čísla svým účastníkům, formuloval žádost o souhlas určenou účastníkovi tak, aby vyjádřil svůj souhlas zvlášť podle toho, do jakého členského státu mohou být údaje předány.[366]

Jednoznačný souhlas

Souhlas musí být vždy udělen jednoznačně.[367] To znamená, že by neměly existovat důvodné pochybnosti o tom, že subjekt údajů chtěl vyjádřit souhlas se zpracováním svých údajů. Například nečinnost subjektu údajů neznamená jednoznačný souhlas.

363 Rozsudek SDEU ze dne 15. března 2017, C-536/15, *Tele2 (Netherlands) BV a další v. Autoriteit Consument en Markt (AMC)*.

364 Směrnice Evropského parlamentu a Rady 2002/22/ES ze dne 7. března 2002 o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), Úř. věst. 2002 L 108, s. 51, ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, (směrnice o univerzální službě), Úř. věst. 2009 L 337, s. 11.

365 Rozsudek SDEU ze dne 15. března 2017, C-536/15, *Tele2 (Netherlands) BV a další v. Autoriteit Consument en Markt (AMC)*, bod 36.

366 Tamtéž, body 40–41.

367 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 11.

Tak tomu bude v případě správce, který získal souhlas tím, že ve svých zásadách zachování důvěrnosti uvádí například: „Tím, že používáte naši službu, souhlasíte se zpracováním svých osobních údajů." V takovém případě je možné, že správci budou muset zajistit, aby uživatelé manuálně a jednotlivě s těmito politikami souhlasili.

Pokud je souhlas udělen písemně a tento dokument je součástí smlouvy, musí být souhlas se zpracováním osobních údajů individualizovaný a každopádně „by mělo být pomocí záruk zajištěno, že si je subjekt údajů vědom toho, že dává souhlas a v jakém rozsahu".[368]

Požadavky na souhlas v případě dětí

GDPR stanoví zvláštní ochranu dětí v souvislosti s poskytováním služeb informační společnosti, protože „si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů".[369] Proto podle **práva EU**, pokud poskytovatelé služeb informační společnosti zpracovávají osobní údaje dětí mladších 16 let věku na základě souhlasu, bude toto zpracování zákonné „pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti".[370] Členské státy mohou ve vnitrostátním právu stanovit nižší věkovou hranici, ne však nižší než 13 let.[371] Souhlas osoby, která vykonává rodičovskou zodpovědnost, není nutný „v případě preventivních či poradenských služeb nabízených přímo dětem".[372] Informace a sdělení určené dětem by měly být podávány za použití jasných a jednoduchých jazykových prostředků, aby jim děti snadno porozuměly.[373]

Právo kdykoliv souhlas odvolat

GDPR zahrnuje obecné právo kdykoliv souhlas odvolat.[374] Subjekt údajů musí být informován o tomto právu předtím, než udělí souhlas, a může toto své právo

368 Tamtéž, 42. bod odůvodnění.

369 Tamtéž, 38. bod odůvodnění.

370 Tamtéž, čl. 8 odst. 1 první odrážka. Pojem „služby informační společnosti" je vymezen v čl. 4 bodu 25 obecného nařízení o ochraně osobních údajů.

371 Obecné nařízení o ochraně osobních údajů, čl. 8 odst. 1 druhá odrážka.

372 Tamtéž, 38. bod odůvodnění.

373 Tamtéž, 58. bod odůvodnění. Viz také Modernizovanou úmluvu č. 108, čl. 15 odst. 2 písm. e). Vysvětlující zpráva k Modernizované úmluvě č. 108, body 68 a 125.

374 Obecné nařízení o ochraně osobních údajů, čl. 7 odst. 3. Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 45.

vykonávat podle svého uvážení. Nemělo by být nutné uvádět důvody pro odvolání souhlasu a nemělo by hrozit žádné riziko nepříznivých důsledků na rámec ukončení požívání výhod, které mohou plynout z užívání údajů, které bylo dohodnuto předem. Odvolání souhlasu by mělo být stejně snadné jako jeho poskytnutí.[375] Souhlas nemůže být svobodný, pokud subjekt údajů není schopen souhlas odvolat, aniž by byl poškozen, nebo pokud není stejně snadné souhlas odvolat jako jej poskytnout.[376]

Příklad: Zákazník souhlasí s tím, že bude přijímat reklamní poštovní zásilky na adresu, kterou poskytne správci údajů. Pokud zákazník souhlas odvolá, musí správce okamžitě zastavit zasílání reklamních poštovních zásilek. Neměly by existovat žádné důsledky trestající zákazníka, například pokuty. Odvolání souhlasu se však vykonává do budoucna a nemá retroaktivní účinek. Období, kdy byly zákazníkovy osobní údaje zpracovávány zákonně – díky souhlasu zákazníka –, bylo legitimní. Odvolání souhlasu brání jakémukoliv dalšímu zpracování těchto údajů, ledaže je toto zpracování v souladu s právem na výmaz.[377]

Nezbytnost pro splnění smlouvy

Podle práva EU stanoví čl. 6 odst. 1 písm. b) GDPR další základ pro legitimní zpracování, totiž pokud je zpracování „nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů". Toto ustanovení zahrnuje rovněž předsmluvní vztahy. Například v případech, kdy jedna smluvní strana má v úmyslu uzavřít smlouvu, ale dosud tak neučinila, třeba proto, že ještě zbývá provést určité kontroly. Pokud jedna smluvní strana musí zpracovávat údaje za tímto účelem, je toto zpracování legitimní, pokud je „nezbytné pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů".[378]

Pojem zpracování osobních údajů jako „legitimní[ho] základ[u] stanovené[ho] právními předpisy" v čl. 5 odst. 2 Modernizované úmluvy č. 108 rovněž zahrnuje

375 Obecné nařízení o ochraně osobních údajů, čl. 7 odst. 3.

376 Viz obecné nařízení o ochraně osobních údajů, 42. bod odůvodnění; Vysvětlující zprávu k Modernizované úmluvě č. 108, bod 42.

377 Obecné nařízení o ochraně osobních údajů, čl. 17 odst. 1 písm. b).

378 Tamtéž, čl. 6 odst. 1 písm. b).

„zpracování údajů za účelem splnění smlouvy (nebo předsmluvních opatření na žádost subjektu údajů), jíž je subjekt údajů smluvní stranou".[379]

Právní povinnosti správce

Právo EU stanoví další důvod pro legitimní zpracování údajů, tj. pokud „je [zpracování] nezbytné pro splnění právní povinnosti, která se na správce vztahuje" (čl. 6 odst. 1 písm. c) GDPR). Toto ustanovení se týká správců působících jak v soukromém, tak ve veřejném sektoru; právní povinnosti správců údajů z veřejného sektoru mohou také spadat do působnosti čl. 6 odst. 1 písm. e) GDPR. Existuje řada příkladů situací, kdy právo ukládá správcům v soukromém sektoru zpracovávat údaje o konkrétních subjektech údajů. Zaměstnavatelé musejí například zpracovávat údaje o svých zaměstnancích pro účely sociálního zabezpečení a zdanění a podniky musí zpracovávat údaje o svých zákaznících pro daňové účely.

Právní povinnost může vyplývat z práva Unie nebo práva členských států, které by mohlo být základem pro jednu nebo několik operací zpracování. Účel zpracování, stanovení podrobností týkajících se určení správce, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje sdělit, účelového omezení, doby uložení a dalších opatření k zajištění zákonného a spravedlivého zpracování by měl být stanoven právním předpisem.[380] Každý takový právní předpis, který je základem pro zpracování osobních údajů, musí být v souladu jak s články 7 a 8 Listiny, tak s článkem 8 EÚLP.

Právní povinnosti správce rovněž slouží jako základ pro legitimní zpracování údajů **podle práva RE**.[381] Jak bylo uvedeno dříve, právní povinnosti správců v soukromém sektoru jsou pouze jedním zvláštním případem oprávněných zájmů dalších osob, jak je uvedeno v čl. 8 odst. 2 EÚLP. Příklad, kdy zaměstnavatel zpracovává údaje o svých zaměstnancích je proto relevantní i pro právo RE.

379 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 46; Rada Evropy, Výbor ministrů (2010): Doporučení CM/Rec(2010)13 Výboru ministrů členským státům o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů v kontextu profilování, 23. listopadu 2010, čl. 3.4 písm. b).

380 Obecné nařízení o ochraně osobních údajů, 45. bod odůvodnění.

381 Rada Evropy, Výbor ministrů (2010): Doporučení CM/Rec(2010)13 Výboru ministrů členským státům o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů v kontextu profilování, 23. listopadu 2010, čl. 3.4 písm. a).

Životně důležité zájmy subjektu údajů nebo jiné fyzické osoby

Podle práva EU stanoví čl. 6 odst. 1 písm. d) GDPR, že zpracování osobních údajů je zákonné, pokud „je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby". Tento legitimní důvod může být uplatněn pouze pro zpracování osobních údajů na základě životně důležitých zájmů jiné fyzické osoby, pokud toto zpracování „zjevně nemůže být založeno na jiném právním základě".[382] Někdy může být jistý druh zpracování založen na důvodech veřejného zájmu i životně důležitých zájmů subjektu údajů nebo jiné osoby. Tak je tomu například při monitorování epidemie a jejího vývoje, nebo pokud dojde k nouzové humanitární situaci.

V právu RE nejsou životně důležité zájmy subjektu údajů uvedeny v článku 8 EÚLP. Má se však za to, že životně důležité zájmy subjektu údajů jsou implikovány v pojmu „legitimní základ" uvedeném v čl. 5 odst. 2 Modernizované úmluvy č. 108, který se týká legitimity zpracování osobních údajů.[383]

Veřejný zájem a výkon veřejné moci

Vzhledem k tomu, že veřejné záležitosti je možné uspořádat řadou různých způsobů, stanoví čl. 6 odst. 1 písm. e) GDPR, že osobní údaje mohou být zákonně zpracovávány, pokud „je [zpracování] nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce[...]".[384]

Příklad: Ve věci *Huber v. Bundesrepublik Deutschland*[385] pan Huber, rakouský státní příslušník pobývající v Německu, požádal Spolkový úřad pro migraci a uprchlíky, aby odstranil údaje, které se jej týkají, z centrálního registru cizinců (dále jen „AZR"). Tento registr, který obsahuje osobní údaje státních příslušníků EU, kteří nejsou Němci, ale pobývají v Německu po dobu delší než tři měsíce, se používá pro statistické účely nebo jej používají donucovací a soudní orgány při vyšetřování a stíhání trestné činnosti nebo osob, které ohrožují veřejnou bezpečnost. Předkládající soud se ptal, zda je zpracování osobních údajů, které je prováděno v takovém centrálním registru cizinců

382 Obecné nařízení o ochraně osobních údajů, 46. bod odůvodnění.

383 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 46.

384 Viz obecné nařízení o ochraně osobních údajů, 45. bod odůvodnění.

385 Rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*.

– do něhož mají přístup i jiné orgány veřejné moci– slučitelné s právem EU vzhledem k tomu, že pro německé státní příslušníky žádný takový registr neexistuje.

SDEU rozhodl, že podle čl. 7 písm. e) směrnice 95/46/ES[386] může být zpracování osobních údajů oprávněné, pokud je nezbytné pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci.

Podle SDEU „[s] ohledem na cíl spočívající v zajištění rovnocenné úrovně ochrany ve všech členských státech tudíž nemůže mít pojem „nezbytnost", jak vyplývá z čl. 7 písm. e) směrnice 95/46/ES[387] […], rozdílný obsah v jednotlivých členských státech. Jedná se tedy o autonomní pojem práva Společenství, který musí být vykládán tak, aby plně odpovídal předmětu této směrnice, jak je definován v jejím čl. 1 odst. 1."[388]

SDEU konstatoval, že právo volného pohybu občanů Unie na území členského státu, jehož nejsou státními příslušníky, není bezpodmínečné, nýbrž s ním mohou být spojena omezení a podmínky stanovené ve Smlouvě o založení Evropského společenství, jakož i v předpisech přijatých k jejímu provedení. Je tedy v zásadě legitimní, aby členský stát používal registr, jako je AZR, na podporu orgánů odpovědných za provádění právních předpisů v souvislosti s právem pobytu, takový registr nesmí obsahovat jiné informace než ty, které jsou za tímto konkrétním účelem nezbytné. SDEU dospěl k závěru, že systém zpracování osobních údajů je v souladu s právem EU, pouze pokud obsahuje údaje nezbytné k provádění této právní úpravy a pokud jeho centralizovaná povaha umožňuje účinnější provádění této právní úpravy. Vnitrostátní soud musí ověřit, zda byly tyto podmínky splněny v tomto konkrétním případě. Pokud ne, nelze uchovávání a zpracovávání osobních údajů v registru, jako je AZR, pro statistické účely považovat na jakémkoliv základě za nezbytné ve smyslu čl. 7 písm. e)[389] směrnice 95/46/ES.[390]

386 Někdejší směrnice o ochraně údajů, čl. 7 písm. e), nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. e).

387 Tamtéž.

388 Rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, bod 52.

389 Někdejší směrnice o ochraně údajů, čl. 7 písm. e), nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. e).

390 Rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, body 54, 58–59 a 66–68.

V neposlední řadě pak, pokud jde o otázku používání údajů obsažených v registru za účelem boje proti trestné činnosti, SDEU rozhodl, že tento cíl „nutně zahrnuje stíhání spáchaných trestných činů a deliktů bez ohledu na státní příslušnost jejich pachatelů". Dotčený registr neobsahuje osobní údaje týkající se státních příslušníků dotčených členských států a toto rozdílné zacházení představuje diskriminaci, kterou zakazuje článek 18 SFEU. SDEU tudíž dospěl k závěru, že toto ustanovení „brání tomu, aby členský stát zavedl s cílem bojovat proti trestné činnosti systém zpracování osobních údajů, který se týká výlučně občanů Unie, kteří nejsou státními příslušníky tohoto členského státu".[391]

Použití osobních údajů orgány jednajícími ve veřejné sféře se také musí řídit článkem 8 **EÚLP** a má se na ně v příslušných případech vztahovat čl. 5 odst. 2 Modernizované úmluvy č. 108.[392]

Oprávněné zájmy správce nebo třetí strany

Podle **práva EU** nemá oprávněné zájmy pouze subjekt údajů. Článek 6 odst. 1 písm. f) GDPR stanoví, že osobní údajů mohou být zákonně zpracovány pouze tehdy, pokud „je [to] nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany [s výjimkou orgánů veřejné moci při plnění jejich úkolů], kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu [...]".[393]

Existence oprávněného zájmu musí být pečlivě posouzena v každém jednotlivém případě.[394] Pokud jsou zjištěny oprávněné zájmy správce, pak je třeba vyvažovat mezi těmito zájmy a zájmy nebo základními právy a svobodami subjektu údajů.[395] Při takovém posuzování je třeba zvážit přiměřená očekávání subjektu údajů s cílem určit, zda zájmy správce převažují nad zájmy nebo základními právy subjektu údajů.[396] Pokud práva subjektu údajů převáží nad oprávněnými zájmy správce, pak

391 Tamtéž, body 78 a 81.

392 Vysvětlující zpráva k Modernizované úmluvě č. 108, body 46 a 47.

393 Oproti směrnici 95/46/ES nabízí obecné nařízení o ochraně osobních údajů více příkladů případů, které se považují za oprávněný zájem.

394 Obecné nařízení o ochraně osobních údajů, preambule, 47. bod odůvodnění.

395 Pracovní skupina zřízená podle článku 29 (2014), *Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES*, 4. dubna 2014.

396 Tamtéž.

může správce přijmout opatření a provést záruky s cílem zajistit, že dopad na práva subjektu údajů bude minimalizován (například pseudonymizace údajů), a zvrátit „rovnováhu", než se bude moci v souladu se zákonem odvolávat na tento legitimní základ pro zpracování. Ve svém stanovisku k pojmu oprávněných zájmů správce údajů pracovní skupina zřízená podle článku 29 zdůraznila stěžejní úlohu odpovědnosti a transparentnosti a práv subjektu údajů podat námitku proti zpracování jejich údajů nebo proti přístupu k nim, jejich změně, výmazu nebo předání, při hledání rovnováhy mezi oprávněnými zájmy správce a zájmy základních práv subjektu údajů.[397]

V bodech odůvodnění GDPR je uvedeno několik příkladů toho, co představuje oprávněný zájem dotčeného správce údajů. Například je povoleno zpracování osobních údajů bez souhlasu subjektu údajů, pokud se provádí pro účely přímého marketingu nebo pokud je takové zpracování „nezbytně nutné pro účely zamezení podvodům".[398]

Ve své judikatuře SDEU tuto zkoušku dále rozpracoval s cílem určit, co představuje legitimní zájem.

Příklad: Věc *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] se týkala škody na trolejbusu dopravní společnosti Rīgas, kterou způsobil cestující, který nečekaně otevřel dveře vozidla taxislužby. Společnost Rīgas satiksme chtěla cestujícího žalovat o náhradu škody. Jméno cestujícího však mohla sdělit pouze policie a ta odmítla předat číslo průkazu totožnosti a adresu cestujícího a namítla, že sdělení těchto údajů by bylo nezákonné podle vnitrostátních právních předpisů o ochraně osobních údajů.

Předkládající lotyšský soud požádal SDEU, aby rozhodl o předběžné otázce, zda právní předpisy EU v oblasti ochrany údajů ukládají povinnost zveřejnit veškeré osobní údaje nutné k zahájení občanskoprávního řízení proti osobě, která je údajně zodpovědná za přestupek.[400]

397 Tamtéž.

398 Obecné nařízení o ochraně osobních údajů, preambule, 47. bod odůvodnění.

399 Rozsudek SDEU ze dne 4. května 2017, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme"*.

400 Tamtéž, bod 23.

SDEU objasnil, že právo EU v oblasti ochrany údajů zahrnuje možnost – nikoliv povinnost – sdělit údaje osobě za účelem uskutečnění oprávněných zájmů, které daná strana sleduje.[401] SDEU stanovil tři kumulativní podmínky, které musí být splněny, aby bylo zpracování osobních údajů zákonné na základě „oprávněných zájmů".[402] Zaprvé, třetí strana, jíž byly údaje sděleny, musí sledovat oprávněný zájem. To v tomto konkrétním případě znamená, že žádost o osobní informace za účelem podání žaloby na danou osobu kvůli způsobení majetkové škody představuje legitimní zájem třetí strany. Zadruhé, zpracování osobních údajů musí být nezbytné pro účely oprávněných zájmů, které jsou sledovány. V této věci je získání osobních informací, jako je adresa a/nebo identifikační číslo, naprosto nezbytné k identifikaci dané osoby. Zatřetí, základní práva a svobody subjektu údajů nesmí mít přednost před oprávněnými zájmy správce nebo třetích stran. Vyvažování zájmů je třeba provádět individuálně pro každý případ a s ohledem na prvky, jako je závažnost zásahu do práv subjektu údajů, nebo za určitých okolností dokonce věku subjektu údajů. V této konkrétní věci se však SDEU domníval, že je odmítnutí sdělit údaje odůvodněné jen proto, že subjekt údajů je nezletilá osoba.

V rozsudku *ASNEF a FECEMD* SDEU výslovně rozhodl o zpracování údajů na zákonném základě „oprávněných zájmů", který byl v té době zakotven v čl. 7 písm. f) směrnice o ochraně údajů.[403]

Příklad: Ve věci *ASNEF a FECEMD*[404] SDEU objasnil, že vnitrostátní právo nemůže přidávat podmínky k těm, které jsou uvedeny v čl. 7 písm. f) směrnice a jež se týkají zákonného zpracování údajů.[405] Věc se týkala situace, kdy španělské právo na ochranu údajů obsahovalo ustanovení, podle kterého se mohly jiné soukromé subjekty odvolávat na oprávněný zájem při zpracování osobních údajů, pouze pokud byly dotčené informace již uvedeny ve veřejných zdrojích.

401 Tamtéž, bod 26.

402 Tamtéž, body 28–34.

403 Někdejší směrnice o ochraně osobních údajů, čl. 7 písm. f), nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. f).

404 Rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*.

405 Někdejší směrnice o ochraně osobních údajů, čl. 7 písm. f), nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. f).

SDEU nejprve konstatoval, že směrnice 95/46/ES[406] má zajistit, aby byla úroveň ochrany práv a svobod jednotlivých osob, pokud jde o zpracování osobních údajů, rovnocenná ve všech členských státech. Sblížení vnitrostátních právních předpisů platných v této oblasti také nesmí vést k oslabení ochrany, kterou zajišťují. Musí mít naopak za cíl zajištění vysoké úrovně ochrany v EU.[407] SDEU proto rozhodl, že „[z] cíle spočívajícího v zajištění rovnocenné úrovně ochrany ve všech členských státech [...] vyplývá, že článek 7 směrnice 95/46/ES[408] stanoví taxativní a omezující výčet případů, v nichž lze zpracování osobních údajů považovat za zákonné". Kromě toho „členské státy nemohou doplnit nové zásady pro oprávněné zpracování osobních údajů, obsažené v článku 7 směrnice 95/46/ES[409], ani upravovat další požadavky, které by pozměnily dosah některé ze šesti zásad zakotvených" v článku 7.[410] SDEU připustil, že v souvislosti s vyvažováním, které je nezbytné podle čl. 7 písm. f) směrnice 95/46/ES, je možné zohlednit, že závažnost zásahu do základních práv subjektu dotčeného uvedeným zpracováním údajů se může lišit v závislosti na skutečnosti, zda jsou dotčené údaje již uvedeny ve veřejně přístupných zdrojích, či nikoli.

Avšak čl. 7 písm. f) směrnice „brání tomu, aby členský stát vyloučil kategorickým a obecným způsobem možnost zpracování určitých kategorií osobních údajů a neumožnil vyvážení proti sobě stojících práv a zájmů v konkrétním případě".

S ohledem na tyto úvahy dospěl SDEU k závěru, že čl. 7 písm. f) směrnice 95/46/ES[411] musí být vykládán v tom smyslu, že „brání vnitrostátní právní úpravě, která v případě, že není dán souhlas subjektu údajů, vyžaduje k umožnění zpracování jeho osobních údajů, které je nezbytné pro uskutečnění oprávněného zájmu správce tohoto zpracování nebo třetí osoby či

406 Někdejší směrnice o ochraně osobních údajů, nyní obecné nařízení o ochraně osobních údajů.

407 Rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, bod 28. Viz směrnici o ochraně osobních údajů, 8. a 10. bod odůvodnění.

408 Někdejší směrnice o ochraně osobních údajů, článek 7, nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. f).

409 Někdejší směrnice o ochraně osobních údajů, článek 7, nyní obecné nařízení o ochraně osobních údajů, článek 6.

410 Tamtéž.

411 Někdejší směrnice o ochraně osobních údajů, čl. 7 písm. f), nyní obecné nařízení o ochraně osobních údajů, čl. 6 odst. 1 písm. f).

třetích osob, jimž jsou tyto údaje sdělovány, aby kromě dodržení základních práv a svobod subjektu údajů byly tyto údaje uvedeny ve veřejně přístupných zdrojích, a tím tedy kategoricky a obecným způsobem vylučuje jakékoli zpracování údajů, které nejsou v takových zdrojích uvedeny"[412].

Kdykoliv jsou osobní údaje zpracovány na základě „oprávněných zájmů", má jednotlivec právo kdykoliv vznést námitku ke zpracování z důvodů týkajících se jeho konkrétní situace v souladu s čl. 21 odst. 1 GDPR. Správce musí ukončit zpracování, pokud neprokáže závažné oprávněné důvody pro pokračování zpracovávání.

Pokud jde o **právo RE**, lze nalézt podobné formulace v Modernizované úmluvě č. 108[413] a v doporučeních RE. Doporučení o profilování uznává zpracování osobních údajů pro účely profilování jako legitimní, pokud je nezbytné pro naplňování oprávněných zájmů jiných osob, „kromě případů, kdy jsou těmto zájmům nadřazena základní práva a svobody subjektů údajů".[414] Kromě toho je „ochrana práv a svobod jiných" uvedena v čl. 8 odst. 2 EÚLP jako jeden z oprávněných důvodů pro omezení práva na ochranu údajů.

Příklad: Ve věci *Y v. Turecko*[415] byl stěžovatel HIV pozitivní. Protože byl při příjezdu do nemocnice v bezvědomí, informovala posádka sanitky zaměstnance nemocnice, že pacient je HIV pozitivní. Stěžovatel namítal před ESLP, že zveřejnění této informace bylo porušením jeho práva na respektování soukromého života. Avšak vzhledem k nutnosti chránit bezpečnost zaměstnanců nemocnice nebylo toto sdílení informací považováno za porušení jeho práv.

412 Rozsudek SDEU ze dne 24. listopadu 2011, spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, body 40, 44 a 48–49.

413 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 46.

414 Rada Evropy, Výbor ministrů (2010): Doporučení CM/Rec(2010)13 a důvodová zpráva o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů v kontextu profilování, 23. listopadu 2010, čl. 3.4 písm. b) (doporučení o profilování).

415 Rozsudek ESLP z dne 17. února 2015, *Y. v. Turecko*, č. 648/10.

4.1.2. Zpracování zvláštní kategorií údajů (citlivé osobní údaje)

Právo RE ponechává stanovení vhodných způsobů ochrany pro používání citlivých osobních údajů na vnitrostátním právu, pokud budou splněny podmínky stanovené v článku 6 Modernizované úmluvy č. 108, tedy že budou v právních předpisech zakotveny vhodné záruky, které doplňují záruky stanovené touto Úmluvou. **Právo EU** v článku 9 GDPR uvádí podrobný režim pro zpracování zvláštních kategorií údajů (takzvané „citlivé osobní údaje"). Tyto údaje vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení a členství v odborech. Dále uvádějí režim pro zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Zpracování citlivých osobních údajů je v zásadě zakázáno.[416]

Existuje však taxativní seznam výjimek z tohoto zákazu, který lze nalézt v čl. 9 odst. 2 tohoto nařízení a který představuje zákonné důvody pro zpracování citlivých osobních údajů. Mezi tyto výjimky patří situace, kdy:

- subjekt údajů udělí výslovný souhlas se zpracováním osobních údajů,
- zpracování provádí v rámci svých oprávněných činností neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a vztahuje se pouze na (bývalé) členy nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli,
- zpracování se týká osobních údajů výslovně zveřejněných subjektem údajů,
- zpracování je nezbytné:
  - pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany,
  - pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (v případě, že subjekt údajů nemůže udělit souhlas),

416 Někdejší směrnice o ochraně osobních údajů, čl. 7 písm. f), nyní obecné nařízení o ochraně osobních údajů, čl. 9 odst. 1.

- pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí,

- pro účely preventivního nebo pracovního lékařství: „pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem“,

- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,

- z důvodů veřejného zájmu v oblasti veřejného zdraví nebo

- z důvodů významného veřejného zájmu.

Ke zpracování zvláštních kategorií údajů se tudíž smluvní vztah se subjektem údajů nepovažuje za právní základ oprávněného zpracování citlivých osobních údajů, a to kromě smlouvy se zdravotnickým pracovníkem podléhající povinnosti zachovávat služební tajemství.[417]

Výslovný souhlas subjektu údajů

Podle **práva EU** je prvním možným důvodem pro zákonné zpracování jakýchkoliv údajů, bez ohledu na to, zda jsou citlivé, či nikoliv, souhlas subjektu údajů. V případě citlivých osobních údajů musí být tento souhlas výslovný. Právo Unie nebo členského státu však může stanovit, že jednotlivec nemůže zrušit zákaz zpracování zvláštních kategorií údajů.[418] Tak tomu může být například v situaci, kdy zpracování obnáší pro subjekt údajů neobvyklá rizika.

Pracovní právo nebo právo v oblasti sociálního zabezpečení a sociální ochrany

Podle **práva EU** je možné zákaz podle čl. 9 odst. 1 zrušit, pokud je zpracování nezbytné pro plnění povinností a výkon práv správce subjektu údajů v oblasti zaměstnanosti nebo sociálního zabezpečení. Zpracování však musí být povoleno

417 Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. h) a i).

418 Tamtéž, čl. 9 odst. 2 písm. a).

právem EU, vnitrostátním právem nebo kolektivní dohodou podle vnitrostátního práva, které stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů.[419] Záznamy o zaměstnancích v držení dané organizace mohou obsahovat citlivé osobní údaje za určitých podmínek stanovených v GDPR a v příslušném vnitrostátním právu. K příkladům citlivých osobních údajů může patřit členství v odborech nebo zdravotnické informace.

Životně důležité zájmy subjektu údajů nebo jiné osoby

Podle **práva EU** je možné zpracovávat citlivé osobní údaje stejně jako v případě jiných údajů z důvodu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.[420] Pokud je zpracování založeno na životně důležitých zájmech jiné osoby, je možné se na tento oprávněný důvod odvolávat, pouze pokud toto zpracování „zjevně nemůže být založeno na jiném právním základě".[421] V některých případech může zpracování osobních údajů chránit zájmy jednotlivce i veřejné zájmy, například v případě zpracování nezbytného pro humanitární účely.[422]

Aby bylo zpracování citlivých osobních údajů na tomto základě oprávněné, musí být nemožné požádat subjekt údajů o souhlas, protože například je subjekt údajů v bezvědomí nebo není přítomen a není možné se s ním spojit. Jinými slovy, daná osoba není schopna z fyzických nebo právních důvodů udělit souhlas.

Charitativní organizace či neziskové subjekty

Zpracovat osobní údaje mohou při provádění svých oprávněných činností také nadace, sdružení nebo jiné neziskové subjekty, které sledují politické, filozofické, náboženské nebo odborové cíle. Zpracování se však musí týkat výlučně současných nebo bývalých členů tohoto subjektu nebo osob, které s ním udržují pravidelné styky.[423] Citlivé osobní údaje nemohou být sdělovány osobám mimo tyto subjekty bez souhlasu subjektu údajů.

419 Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. b).

420 Tamtéž, čl. 9 odst. 2 písm. c).

421 Tamtéž, 46. bod odůvodnění.

422 Tamtéž.

423 Tamtéž, čl. 9 odst. 2 písm. d).

Údaje zjevně zveřejněné subjektem údajů

Článek 9 odst. 2 písm. e) GDPR stanoví, že zpracování není zakázáno, pokud se týká údajů zjevně zveřejněných subjektem údajů. Ačkoliv význam slov „zjevně zveřejněné subjektem údajů" není v nařízení definován, jelikož se jedná o výjimku ze zákazu zpracování citlivých osobních údajů, je třeba chápat úzce a v tom smyslu, že vyžaduje, aby subjekt údajů své osobní údaje zveřejnil záměrně. Tudíž v případě, kdy televize vysílá videozáznam pořízený monitorovací videokamerou mimo jiné zobrazující hasiče, který se zranil během úsilí o evakuaci budovy, není možné mít za to, že dotčený hasič své údaje zjevně zveřejnil. Na druhé straně pokud se tento hasič rozhodne, že popíše událost a zveřejní videozáznam nebo fotografie na veřejné webové stránce, záměrně a zjevně potvrdí, že zveřejňuje své osobní údaje. Je důležité konstatovat, že zveřejnění vlastních údajů nepředstavuje souhlas, ale jedná se o jiné svolení se zpracováním zvláštních kategorií údajů.

Skutečnost, že subjekt údajů zpracovávané osobní údaje zveřejnil, nezprošťuje správce povinností podle práva v oblasti ochrany údajů. Například se na osobní údaje i nadále uplatňuje zásada účelového omezení, i když tyto údaje byly veřejně dostupné.[424]

Právní nároky

Zpracování zvláštních kategorií údajů, které je „nezbytné pro určení, výkon nebo obhajobu právních nároků", ať už v rámci soudního řízení, nebo správního a mimosoudního řízení,[425] není podle GDPR dovoleno.[426] V tomto případě musí být zpracování relevantní pro konkrétní právní nárok a případně jeho výkon nebo obhajobu a může o ně požádat kterákoliv ze stran sporu.

Soudy jednající v rámci svých soudních pravomocí mohou zpracovávat zvláštní kategorie údajů v souvislosti s řešením právního sporu.[427] K příkladům těchto zvláštních kategorií údajů zpracovávaných v tomto kontextu mohou patřit třeba genetické údaje při určování rodičovství nebo zdravotní stav, pokud se některé důkazy týkají podrobností o zranění, které utrpěla oběť trestného činu.

424 Pracovní skupina zřízená podle článku 29 (2013), *Stanovisko 3/2013 k účelovému omezení*, WP 203, Brusel, 2. dubna 2013, s. 14.

425 Obecné nařízení o ochraně osobních údajů, preambule, 52. bod odůvodnění.

426 Tamtéž, čl. 9 odst. 2 písm. f).

427 Tamtéž.

Důvody významného veřejného zájmu

Podle čl. 9 odst. 2 písm. g) GDPR mohou členské státy zavést další okolnosti, kdy mohou být osobní citlivé údaje zpracovávány, pokud:

- zpracování je nezbytné z důvodu významného veřejného zájmu,
- je stanoveno na základě evropského nebo vnitrostátního práva,
- evropské nebo vnitrostátní právo je přiměřené, dodržuje právo na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.[428]

Významným příkladem jsou elektronické systémy zdravotní evidence. Díky těmto systémům mohou být zdravotní údaje shromážděné poskytovateli zdravotní péče při ošetřování pacienta dostupné jiným poskytovatelům zdravotní péče tohoto pacienta ve velkém měřítku, obvykle v rámci celého státu.

Pracovní skupina podle článku 29 dospěla k závěru, že zřizování těchto systémů není možné podle stávajících právních předpisů pro zpracování údajů o pacientech.[429] Je však možné, aby elektronické systémy zdravotní evidence existovaly, pokud jsou založeny na „důvodech významného veřejného zájmu".[430] K tomu je zapotřebí výslovný právní základ pro jejich zřizování, který by také obsahoval nezbytné záruky k zajištění, že systém bude bezproblémově fungovat.[431]

Jiné důvody pro zákonné zpracování citlivých osobních údajů

GDPR stanoví, že citlivé osobní údaje mohou být zpracovávány, pokud je zpracování nezbytné:[432]

- pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo

428 Tamtéž, čl. 9 odst. 2 písm. g).

429 Pracovní skupina zřízená podle článku 29 (2007), Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR), WP 131, Brusel, 15. února 2007. Viz také obecné nařízení o ochraně osobních údajů, čl. 9 odst. 3.

430 Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. g).

431 Pracovní skupina zřízená podle článku 29 (2007), Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR), WP 131, Brusel, 15. února 2007.

432 Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. h), i) a j).

sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva EU nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem,

- z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva EU nebo členského státu. Právní řád musí poskytnout vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů,

- pro účely archivace, vědeckého či historického výzkumu nebo pro statistické účely na základě práva Unie nebo členského státu. Právo musí být přiměřené sledovanému cíli, dodržovat podstatu práva na ochranu údajů a poskytovat vhodné a konkrétní záruky pro ochranu práv a zájmů subjektu údajů.

Další podmínky podle vnitrostátního práva

GDPR také umožňuje členským státům zavést nebo zachovávat další podmínky, včetně omezení zpracování genetických, biometrických a zdravotních údajů.[433]

4.2. Pravidla zabezpečení zpracování

Hlavní body

- Pravidla zabezpečení zpracování ukládají správci a zpracovateli povinnost zavést vhodná technická a organizační opatření s cílem zabránit neoprávněnému zásahu do operací zpracování údajů.
- Nezbytná úroveň bezpečnosti údajů je určena:
  - bezpečnostními prvky dostupnými na trhu pro každý daný typ zpracování,
  - náklady,
  - riziky, která zpracování údajů představuje pro základní práva a svobody subjektů údajů.
- Zajištění důvěrnosti osobních údajů je součástí obecné zásady uznané v obecném nařízení o ochraně osobních údajů.

433 Tamtéž, čl. 9 odst. 2 písm. h) a čl. 9 odst. 4.

Podle **práva EU i práva RE** mají správci obecnou povinnost chovat se transparentně a nést odpovědnost při zpracování osobních údajů, a zejména pokud jde o porušení zabezpečení osobních údajů, dojde-li k nim. V případě porušení zabezpečení osobních údajů musí správci uvědomit dozorové úřady, ledaže by bylo nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Subjekty údajů by také měly být informovány o porušení zabezpečení osobních údajů, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

4.2.1. Prvky zabezpečení údajů

Podle příslušných ustanovení **práva EU**:

> *„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku […].“*[434]

K těmto opatřením mimo jiné patří:

- pseudonymizace a šifrování osobních údajů,[435]
- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování,[436]
- obnovení dostupnosti osobních údajů a přístupu k nim včas v případě ztráty údajů,[437]
- proces testování, posuzování a hodnocení účinnosti opatření pro zajištění bezpečnosti zpracování.[438]

Podobné ustanovení existuje podle **práva RE**:

434 Tamtéž, čl. 32 odst. 1.

435 Tamtéž, čl. 32 odst. 1 písm. a).

436 Tamtéž, čl. 32 odst. 1 písm. b).

437 Tamtéž, čl. 32 odst. 1 písm. c).

438 Tamtéž, čl. 32 odst. 1 písm. d).

„Každá smluvní strana zajistí, aby správce, a v případech, kdy je to vhodné, i zpracovatel přijal odpovídající bezpečnostní opatření proti rizikům, jako je náhodný nebo neoprávněný přístup k osobním údajům, jejich zničení, ztráta, využití, úprava nebo poskytnutí."[439]

Podle **práva EU a RE** je správce povinen oznámit dozorovým úřadům porušení zabezpečení osobních údajů, které může mít dopad na práva a svobody jednotlivců (viz oddíl 4.2.3).

Často platí také odvětvové, vnitrostátní a mezinárodní normy, které byly vypracovány za účelem zabezpečeného zpracování údajů. Například projekt EU týkající se evropského systému osvědčení o zachování důvěrného charakteru informací (European Privacy Seal, EuroPriSe) zkoumá možnosti certifikace produktů, zejména softwaru, za účelem usnadnění zajišťování souladu s evropským právem v oblasti ochrany údajů. Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) byla zřízena za účelem zvýšení a posilování schopnosti EU, členských států EU a podnikatelské komunity předcházet problémům a incidentům v oblasti bezpečnosti sítí a informací, zabývat se jimi a reagovat na ně.[440] Agentura ENISA pravidelně zveřejňuje analýzy současných bezpečnostních hrozeb a poradenství, jak proti těmto hrozbám zakročit.[441]

Zabezpečení údajů se nedosahuje pouze zavedením správného vybavení – hardwarového a softwarového. Je také zapotřebí vhodných interních organizačních pravidel. Tato interní pravidla by i v ideálním případě měla zahrnovat tyto otázky:

- pravidelné poskytování informací všem zaměstnancům o pravidlech zabezpečení údajů a jejich povinnostech podle práva na ochranu údajů, zejména pokud jde o jejich povinnost zachovávat mlčenlivost,

- jasné rozdělení povinností a jasné vymezení kompetencí v oblastech týkajících se zpracování údajů, zejména pokud jde o rozhodnutí zpracovávat osobní údaje a předávat údaje třetím stranám nebo subjektům údajů,

439 Modernizovaná úmluva č. 108, čl. 7 odst. 1.

440 Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004, Úř. věst. 2013 L 165.

441 Například ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations [Kybernetické zabezpečení a odolnost chytrých vozidel. Osvědčené postupy a doporučení]; ENISA (2016), Security of Mobile Payments and Digital Wallets [Zabezpečení mobilních plateb a digitálních peněženek].

- používat osobní údaje pouze v souladu s pokyny příslušné osoby nebo podle obecně stanovených pravidel,
- ochrana přístupu do prostor a k hardwaru a softwaru správce či zpracovatele, včetně kontrol oprávnění k přístupu,
- zajištění, že oprávnění k přístupu k osobním údajům udělila způsobilá osoba a je k tomu nutná náležitá dokumentace,
- automatizované protokoly o elektronickém přístupu k osobním údajům a pravidelné kontroly těchto protokolů ze strany interní funkce dozoru (tudíž povinnost zaznamenávání všech činností v oblasti zpracování údajů),
- pečlivá dokumentace pro jiné formy sdělování informací než automatizovaný přístup k údajům s cílem prokázat, že nedošlo k žádnému nezákonnému předávání údajů.

Nabízení dostatečné odborné přípravy a vzdělávání v oblasti zabezpečení údajů je také důležitým prvkem účinných bezpečnostních preventivních opatření. Musí být zavedeny postupy ověřování, aby se zajistilo, že vhodná opatření neexistují jen na papíře, ale jsou prováděna a fungují v praxi (například interní nebo externí audity).

K opatřením na zlepšení úrovně zabezpečení správce nebo zpracovatele patří pracovníci pověření ochranou osobních údajů, vzdělávání zaměstnanců na téma bezpečnosti, pravidelné audity, testy penetrace a pečeti kvality.

Příklad: Ve věci *I. v. Finsko*[442] nebyla stěžovatelka schopna dokázat, že k jejím zdravotním záznamům získali neoprávněný přístup jiní zaměstnanci nemocnice, kde pracovala. Její žaloba na porušení práva na ochranu údajů byla tudíž u vnitrostátních soudů zamítnuta. ESLP dospěl k závěru, že došlo k porušení článku 8 EÚLP, protože evidenční systém nemocnice se zdravotními spisy „byl takový, že nebylo možné zpětně objasnit použití záznamů pacientů, protože uváděl pouze pět posledních nahlédnutí, a že tyto informace byly smazány, jakmile byl spis vrácen do archivu". Pro soud bylo rozhodující, že

442 Rozsudek ESLP ze dne 17. července 2008, *I. v. Finsko*, č. 20511/03.

v nemocnici zavedený systém záznamů zjevně nebyl v souladu s právními požadavky stanovenými ve vnitrostátním právu, což je skutečnost, kterou vnitrostátní soudy náležitě nezohlednily.

EU zavedla směrnici o bezpečnosti sítí a informačních systémů (směrnice o bezpečnosti sítí a informací)[443], což je první celounijní právní nástroj v oblasti kybernetické bezpečnosti. Cílem této směrnice je na jedné straně zlepšit kybernetickou bezpečnost na vnitrostátní úrovni a na straně druhé zvýšit úroveň spolupráce v rámci EU. Ukládá rovněž provozovatelům základních služeb (včetně provozovatelů v odvětví energie, zdraví, bankovnictví, dopravy, digitální infrastruktury atd.) a poskytovatelům digitálních služeb povinnost řídit rizika, zajistit zabezpečení svých sítí a informačních systémů a oznamovat bezpečnostní incidenty.

Budoucnost

V září 2017 Evropská komise předložila návrh nařízení, které mělo přepracovat mandát agentury ENISA s ohledem na nové pravomoci a povinnosti této agentury podle směrnice o bezpečnosti sítí a informací. Cílem předloženého návrhu nařízení je rozvíjet úkoly agentury ENISA a posílit její úlohu jako „referenčního místa v kybernetickobezpečnostním ekosystému EU".[444] Předkládaným návrhem nařízení nejsou dotčeny zásady GDPR a posílením nezbytných prvků tvořících evropský systém certifikace kybernetické bezpečnosti by rovněž mělo být posíleno zabezpečení osobních údajů. Souběžně navrhla Evropská komise v září 2017 návrh prováděcího nařízení upřesňujícího prvky, které musí zohlednit poskytovatelé digitálních služeb s cílem zajistit, aby jejich sítě a informační systémy byly zabezpečeny, jak vyžaduje čl. 16 odst. 8 směrnice o bezpečnosti sítí a informací. V době přípravy této příručky stále probíhaly diskuse o obou návrzích.

443 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, Úř. věst. 2016 L 194.

444 Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti"), COM(2017)477, 13. září 2017, s. 6.

4.2.2. Důvěrnost údajů

V rámci práva EU uznává GDPR důvěrnost osobních údajů jako součást jedné obecné zásady.[445] Důvěrnost musí zajistit poskytovatelé veřejně dostupných služeb elektronických komunikací. Také musejí zajistit bezpečnost svých služeb.[446]

Příklad: Zaměstnankyně pojišťovny přijme na svém pracovišti telefonní hovor od osoby, která uvádí, že je jejím klientem, a vyžaduje informace týkající se pojistné smlouvy této osoby.

V souladu s povinností uchovávat údaje klientů v důvěrnosti musí zaměstnankyně uplatnit alespoň minimální bezpečnostní opatření, než sdělí osobní informace. Toho lze dosáhnout například tím, že zaměstnankyně nabídne, že zavolá zpět na telefonní číslo uvedené ve složce klienta.

Podle čl. 5 odst. 1 písm. f) musí být osobní údaje zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“).

Podle článku 32 musí správce a zpracovatel provést technická a organizační opatření, aby zajistili vysokou úroveň bezpečnosti. K těmto opatřením kromě jiného patří pseudonymizace a šifrování osobních údajů, schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, testování a hodnocení účinnosti opatření a schopnost obnovit zpracování v případě fyzického či technického incidentu. Kromě toho dodržování schváleného kodexu chování nebo schváleného mechanismu pro vydávání osvědčení může posloužit jako prvek k doložení souladu se zásadou integrity a důvěrnosti. Kromě toho podle článku 28 GDPR musí smlouva zavazující zpracovatele vůči správci stanovit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

Povinnost zachovávat mlčenlivost se nevztahuje na situace, kdy údaje nabyde určitá osoba jako soukromá osoba, která není zaměstnancem správce ani zpracovatele. V takovém případě se nepoužije článek 32 a 28 GDPR, protože používání osobních

445 Obecné nařízení o ochraně osobních údajů, čl. 5 odst. 1 písm. f).

446 Směrnice o soukromí a elektronických komunikacích, čl. 5 odst. 1.

údajů soukromými osobami je zcela vyňato z působnosti nařízení, pokud toto použití spadá do vymezení takzvané výjimky pro domácnosti.[447] Výjimka pro domácnosti znamená použití osobních údajů „fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti".[448] Od rozhodnutí SDEU ve věci *Bodil Lindqvist*[449] však tato výjimka musí být vykládána v úzkém smyslu, zejména pokud jde o sdělování údajů. Výjimka pro domácnosti se pak zejména nebude vztahovat na zveřejnění osobních údajů neomezenému počtu příjemců na internetu nebo na zpracování údajů, které má profesionální nebo obchodní aspekty (více podrobností k této věci lze nalézt v oddílech 2.1.2, 2.2.2 a 2.3.1).

Dalším aspektem důvěrnosti, kterou upravuje *lex specialis*, je „důvěrný charakter sdělení". Zvláštní pravidla pro zajištění důvěrného charakteru elektronických komunikací podle směrnice o soukromí a elektronických komunikacích ukládají členským státům povinnost, aby zakázaly příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů.[450] Vnitrostátní právo může povolit výjimky z této zásady, avšak pouze z důvodu národní bezpečnosti, obrany, pro prevenci či vyšetřování, a pokud jsou tato opatření nezbytná a přiměřená vhledem ke sledovaným cílům.[451] Tatáž pravidla se uplatní podle budoucího nařízení o soukromí a elektronických komunikacích, avšak oblast působnosti právního aktu o soukromí a elektronických komunikacích bude rozšířena tak, aby nezahrnovala jenom veřejně dostupné služby elektronických komunikací, ale i komunikaci uskutečňovanou prostřednictvím služeb over the top (např. mobilní aplikace).

Podle práva RE je povinnost zachovávat mlčenlivost implikována v pojmu zabezpečení údajů, uvedeném v čl. 7 odst. 1 Modernizované úmluvy č. 108, který se zabývá zabezpečením údajů.

Pro zpracovatele důvěrnost znamená, že nesmějí bez povolení sdělit údaje třetím stranám nebo jiným příjemcům. Od zaměstnanců správce nebo zpracovatele důvěrnost vyžaduje, aby používali osobní údaje pouze v souladu s pokyny svých příslušných nadřízených.

447 Obecné nařízení o ochraně osobních údajů, čl. 2 odst. 2 písm. c).

448 Tamtéž.

449 Rozsudek SDEU ze dne 6. listopadu 2003, C-101/01, *Trestní řízení proti Bodil Lindqvist*.

450 Směrnice o soukromí a elektronických komunikacích, čl. 5 odst. 1.

451 Tamtéž, čl. 15 odst. 1.

Povinnost zachovávat důvěrnost musí být součástí každé smlouvy mezi správci a jejich zpracovateli. Kromě tomu budou správci a zpracovatelé muset přijmout konkrétní opatření ke stanovení právní povinnosti zachovávat důvěrnost ze strany svých zaměstnanců, čehož se obvykle dosáhne zahrnutím doložek o důvěrnosti do pracovní smlouvy zaměstnance.

Porušení povinnosti zachovávat služební tajemství je trestné podle trestního práva v řadě členských států EU a smluvních stran Úmluvy č. 108.

4.2.3. Ohlašování případů porušení zabezpečení osobních údajů

Porušením zabezpečení osobních údajů se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění zpracovávaných osobních údajů.[452] Ačkoliv nové technologie, jako je šifrování, nyní skýtají více možností k zajištění zabezpečení zpracování, jsou případy porušení zabezpečení osobních údajů stále běžným jevem. Příčiny porušení zabezpečení osobních údajů mohou být různé: od náhodné chyby, které se dopustí osoby pracující v dané organizaci s ohledem na vnější hrozby, jako jsou hackeři a organizace kybernetické trestné činnosti.

Porušení zabezpečení osobních údajů může mít negativní důsledky pro právo na soukromí a právo jednotlivců na ochranu údajů, protože tito jednotlivci v důsledku porušení zabezpečení ztratí kontrolu nad svými osobními údaji. Porušení zabezpečení osobních údajů může vést ke krádeži totožnosti nebo podvodům, finančním ztrátám nebo materiálním poškozením, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím a poškození dobrého jména subjektu údajů. V pokynech k ohlašování případů porušení zabezpečení osobních údajů podle nařízení 2016/679 pracovní skupina zřízená podle článku 29 vysvětluje, že porušení zabezpečení může mít tři druhy dopadu na osobní údaje: poskytnutí údajů, ztráta a/nebo změna.[453] Kromě povinnosti přijmout opatření k zajištění zabezpečení zpracování, jak je vysvětleno v oddíle 4.2, je stejně důležité zajistit, aby v případě, že dojde k porušení zabezpečení údajů, se jimi správci zabývali rychle a vhodným způsobem.

452 Obecné nařízení o ochraně osobních údajů, čl. 4 bod 12; viz také: pracovní skupina zřízená podle článku 29 (2017), *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679*, WP 250, 3. října 2017, s. 8.

453 Pracovní skupina zřízená podle článku 29 (2017), *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679*, WP 250, 3. října 2017, s. 6.

Dozorové úřady a osoby si často nejsou vědomy, že došlo k porušení zabezpečení osobních údajů, a to brání jednotlivcům, aby podnikli kroky k ochraně před nepříznivými důsledky. Za účelem stvrzení práv jednotlivců a omezení dopadu případů porušení zabezpečení údajů ukládají **EU a RE** správcům za jistých okolností ohlašovací povinnost.

Podle Modernizované úmluvy **RE** č. 108 musí smluvní strany přinejmenším ukládat správcům povinnost informovat příslušné dozorové úřady o případech porušení zabezpečení osobních údajů, které mohou závažně zasáhnout do práv subjektů údajů. Toto oznámení by mělo být provedeno „bez zbytečného odkladu".[454]

Právo EU stanoví podrobný režim upravující lhůty a obsah ohlášení.[455] Správci tedy musí ohlásit některé případy porušení zabezpečení osobních údajů dozorovým úřadům bez zbytečného odkladu, a je-li to možné, do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděli. Překročí-li 72hodinovou lhůtu, musí být ohlášení doplněno o vysvětlení tohoto zpoždění. Správci jsou zproštěni ohlašovací povinnosti pouze v případě, kdy jsou schopni prokázat, že je nepravděpodobné, že by porušení zabezpečení osobních údajů představovalo riziko pro práva a svobody dotčený osob.

V nařízení se stanoví minimální informace, které musejí být součástí ohlášení, aby mohly dozorové úřady podniknout nezbytné kroky.[456] Ohlášení musí obsahovat alespoň popis povahy daného případu porušení zabezpečení osobních údajů a kategorií a přibližného počtu dotčených subjektů údajů, popis možných důsledků porušení zabezpečení osobních údajů a opatření, která správce provedl s cílem vyřešit nebo zmírnit nepříznivé dopady. Kromě toho je třeba uvést jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, aby příslušné dozorové úřady mohly získat bližší informace, je-li to nutné.

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody jednotlivců, musí správce oznámit toto porušení bez zbytečného odkladu jednotlivcům (subjektům údajů).[457] Oznámení subjektům údajů, včetně popisu porušení zabezpečení osobních údajů, musí být formulováno za použití jasných a jednoduchých jazykových prostředků

454 Modernizovaná úmluva č. 108, čl. 7 odst. 2; Vysvětlující zpráva k Modernizované úmluvě č. 108, body 64–66.

455 Obecné nařízení o ochraně osobních údajů, článek 33 a 34.

456 Tamtéž, čl. 33 odst. 3.

457 Tamtéž, článek 34.

a musí obsahovat informace podobné těm, které jsou požadovány v ohlášení dozorovým úřadům. Za určitých okolností mohou být správci zproštěni povinnosti oznamovat takováto porušení zabezpečení subjektu údajů. Výjimky platí v případě, že správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování. Rovněž mohou správce zprostit povinnosti oznamovat porušení zabezpečení subjektům údajů opatření, která správce přijal po porušení zabezpečení s cílem zajistit, že se již neprojeví poškození práv a svobod subjektů údajů. V neposlední řadě pak, pokud by oznámení vyžadovalo nepřiměřené úsilí ze strany správce, mohou být subjekty údajů o porušení zabezpečení osobních údajů informovány pomocí jiných prostředků, například veřejného oznámení nebo podobných opatření.[458]

Povinnost oznamovat porušení zabezpečení osobních údajů dozorovým úřadům a subjektům údajů je určena správcům. K porušení osobních údajů však může dojít bez ohledu na to, zda zpracování provádí správce nebo zpracovatel. Z tohoto důvodu je zásadní zajistit, aby zpracovatelé byli také povinni oznamovat případy porušení zabezpečení osobních údajů. V tomto případě musí zpracovatelé ohlásit porušení zabezpečení osobních údajů bez zbytečného odkladu správci.[459] Správce je následně odpovědný za ohlášení dozorovým úřadům a dotčeným subjektům údajů podle výše uvedených pravidel a v příslušných lhůtách.

4.3. Pravidla odpovědnosti a prosazování souladu s právními předpisy

Hlavní body

- K zajištění odpovědnosti při zpracování osobních údajů musí správci a zpracovatelé vést záznamy o činnostech zpracování vykonávaných na jejich zodpovědnost a poskytovat je na vyzvání dozorovým úřadům.
- Obecné nařízení o ochraně osobních údajů stanoví několik nástrojů na podporu souladu s právními předpisy:

458 Tamtéž, čl. 34 odst. 3 písm. c).

459 Tamtéž, čl. 33 odst. 2.

  - v některých situacích jmenování pověřenců pro ochranu osobních údajů,
  - provedení posouzení vlivu před zahájením činností zpracování, u nichž je pravděpodobné, že budou představovat velké riziko pro práva a svobody jednotlivců,
  - předchozí konzultace s příslušným dozorovým úřadem, pokud z posouzení vlivu vyplývá, že zpracování představuje rizika, která není možné zmírnit,
  - kodexy chování pro správce a zpracovatele, které upřesňují uplatňování nařízení v různých odvětvích zpracování,
  - mechanismy pro vydávání osvědčení, pečeti a známky.
- Právo RE navrhuje podobné nástroje na prosazování souladu s právními předpisy v Modernizované úmluvě č. 108.

Zásada odpovědnosti je zvlášť důležitá k zaručení prosazování pravidel v oblasti ochrany údajů v Evropě. Správce je odpovědný za dodržování pravidel ochrany údajů a musí být schopen soulad s pravidly prokázat. Odpovědnost by neměla vstupovat do hry teprve až poté, kdy došlo k porušení předpisů. Naopak, správci mají aktivní povinnost dodržovat dostatečné politiky v oblasti správy údajů ve všech fázích zpracování údajů. Evropské právo v oblasti ochrany údajů ukládá správcům povinnost, aby provedli technická a organizační opatření s cílem zajistit, že zpracování se provádí v souladu s právními předpisy, a aby byli schopni tuto skutečnost prokázat. K těmto opatřením patří jmenování pověřenců pro ochranu osobních údajů, vedení záznamů a dokumentace související se zpracováním a provádění posouzení vlivu na soukromí.

4.3.1. Pověřenci pro ochranu osobních údajů

Pověřenci pro ochranu osobních údajů jsou osoby, které poskytují poradenství ohledně souladu s předpisy v oblasti ochrany údajů v rámci organizací, které provádějí zpracování údajů. Jsou „základním kamenem odpovědnosti“, protože usnadňují soulad s předpisy, a současně také vystupují jako prostředníci mezi dozorovými úřady, subjekty údajů a organizací, která je jmenovala.

Podle práva RE ukládá čl. 10 odst. 1 Modernizované úmluvy č. 108 povinnost nést obecnou zodpovědnost správcům a zpracovatelům. K tomu je zapotřebí, aby správci a zpracovatelé přijali veškerá vhodná opatření pro soulad s pravidly v oblasti ochrany údajů stanovenými v úmluvě a aby byli schopni prokázat, že zpracování údajů, nad kterým vykonávají kontrolu, probíhá v souladu s ustanoveními úmluvy. Ačkoliv úmluva nestanoví konkrétní opatření, která by správci a zpracovatelé měli

přijmout, Vysvětlující zpráva k Modernizované úmluvě č. 108 uvádí, že jmenování pověřence pro ochranu osobních údajů je jedním z možných opatření, které pomáhá prokázat soulad. Pověřenci pro ochranu osobních údajů by měli být vybaveni všemi prostředky nezbytnými k výkonu jejich mandátu.[460]

Na rozdíl od práva RE není v **EU** ponecháno jmenování pověřence pro ochranu osobních údajů vždy jen na uvážení správců a zpracovatelů, ale za určitých podmínek je povinné. GDPR uznává, že pověřenec pro ochranu osobních údajů plní klíčovou úlohu v novém systému správy, a obsahuje podrobná ustanovení týkající se jmenování, postavení, povinností a úkolů pověřence.[461]

GDPR stanoví povinnost jmenovat pověřence pro ochranu osobních údajů ve třech zvláštních případech: pokud zpracování provádí orgán veřejné moci či veřejný subjekt, pokud hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo pokud hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.[462] Ačkoliv termíny jako „rozsáhlé systematické monitorování" a „hlavní činnosti" nejsou v nařízení definovány, vydala pracovní skupina zřízená podle článku 29 pokyny, jak by tyto termíny měly být vykládány.[463]

Příklad: Společnosti provozující sociální média a vyhledávače budou pravděpodobně považovány za správce, jejichž operace zpracování vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů. Obchodní model těchto společností je založen na zpracování velkého objemu osobních údajů a společnosti vytvářejí značný zisk tím, že nabízejí cílené reklamní služby a umožňují společnostem reklamu na stránkách. Cílená reklama je způsob umísťování inzerátů na základě demografie a v minulosti uskutečněných nákupů a chování spotřebitelů. Vyžaduje tedy systematické monitorování on-line návyků a chování subjektů údajů.

460 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 87.

461 Obecné nařízení o ochraně osobních údajů, články 37 až 39.

462 Tamtéž, čl. 37 odst. 1.

463 Pracovní skupina zřízená podle článku 29 (2017), *Pokyny týkající se pověřenců pro ochranu osobních údajů*, WP 243 rev.01, naposledy revidováno a přijato dne 5. dubna 2017.

Příklad: Nemocnice nebo zdravotní pojišťovna jsou typickými příklady správců, jejichž činnosti sestávají z rozsáhlého zpracování zvláštních kategorií osobních údajů. Údaje vypovídající o informacích týkajících se zdraví jednotlivce představují zvláštní kategorie osobních údajů podle práva RE i práva EU, a zasluhují tedy posílenou ochranu. Právo EU dále uznává jako zvláštní kategorie genetické a biometrické údaje. Pokud zdravotnická zařízení nebo pojišťovny zpracovávají tyto údaje ve velkém rozsahu, jsou podle GDPR povinny jmenovat pověřence pro ochranu osobních údajů.

Kromě toho čl. 37 odst. 4 GDPR stanoví, že v jiných případech, než jsou tři povinné případy uvedené v čl. 37 odst. 1, mohou nebo, vyžaduje-li to právo Unie nebo členského státu, musí pověřence pro ochranu osobních údajů jmenovat správce nebo zpracovatel nebo sdružení a jiné subjekty zastupující kategorie správců či zpracovatelů.

Žádné jiné organizace právní předpisy nezavazují, aby jmenovaly pověřence pro ochranu osobních údajů. GDPR však stanoví, že se správci a zpracovatelé mohou rozhodnout, že dobrovolně jmenují pověřence pro ochranu osobních údajů, a současně nařízení umožňuje, aby členské státy mohly toto jmenování učinit povinným pro více druhů organizací, než jsou organizace stanovené v nařízení.[464]

Jakmile správce jmenuje pověřence pro ochranu osobních údajů, musí zajistit, aby byl pověřenec „náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů" v dané organizaci.[465] Pověřenec by měl být například zapojen do poskytování poradenství ohledně provádění posouzení vlivu na ochranu osobních údajů a do vytváření a vedení záznamů o činnostech zpracování v dané organizaci. Aby mohl pověřenec pro ochranu osobních údajů účinně plnit své úkoly, musí mu správci a zpracovatelé poskytnout nezbytné zdroje, včetně finančních zdrojů, infrastruktury a vybavení. Další požadavky zahrnují poskytnutí pověřencům pro ochranu osobních údajů dostatku času na plnění jejich úkolů a průběžnou odbornou přípravu, která jim umožní rozvíjet své odborné znalosti a držet krok s veškerým vývojem práva v oblasti ochrany osobních údajů.[466]

464 Obecné nařízení o ochraně osobních údajů, čl. 37 odst. 3 a 4.

465 Tamtéž, čl. 38 odst. 1.

466 Pracovní skupina zřízená podle článku 29 (2017), Pokyny týkající se pověřenců pro ochranu osobních údajů, WP 243 rev.01, naposledy revidováno a přijato dne 5. dubna 2017, bod 3.1.

GDPR stanoví určité základní záruky k zajištění, že pověřenci pro ochranu osobních údajů jednají nezávisle. Správci a zpracovatelé musí zajistit, aby pověřenec pro ochranu osobních údajů při výkonu svých úkolů v souvislosti s ochranou údajů nedostával žádné pokyny od dané společnosti, včetně osob na nejvyšších úrovních vedení. Kromě toho nesmějí být propuštěni ani nijak sankcionováni za plnění svých úkolů.[467] Vezměme si například případ, kdy pověřenec pro ochranu osobních údajů správci nebo zpracovateli poradí, aby provedli posouzení vlivu na ochranu osobních údajů, protože se domnívají, že zpracování bude mít pravděpodobně za následek vyšší riziko pro subjekty údajů. Společnost nesouhlasí s radou pověřence, nepovažuje ji za náležitě podloženou a následně se rozhodne, že posouzení vlivu neprovede. Společnost může radu přehlížet, ale nemůže pověřence propustit nebo sankcionovat za to, že tento postup poradil.

Úkoly a povinnosti pověřenců pro ochranu osobních údajů jsou pak podrobně uvedeny v článku 39 GDPR. Patří k nim mimo jiné povinnost poskytování informací a poradenství společnostem a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle právních předpisů a sledování souladu s právními předpisy EU a členských států v oblasti ochrany údajů prostřednictvím provádění auditů a školení zaměstnanců zapojených do operací zpracování. Pověřenci pro ochranu osobních údajů musejí také spolupracovat s dozorovým úřadem a působit jako kontaktní místo pro tento úřad v záležitostech týkajících se zpracování údajů, například v případě porušení zabezpečení osobních údajů.

Pokud jde o osobní údaje zpracovávané orgány a institucemi EU, nařízení (ES) č. 45/2001 stanoví, že každý orgán a instituce EU musí jmenovat pověřence (inspektora) pro ochranu osobních údajů. Pověřenci pro ochranu osobních údajů se svěřuje povinnost zajistit, že jsou správně prováděna ustanovení tohoto nařízení v rámci orgánů a institucí EU a že subjekty údajů i správci údajů jsou informováni o svých právech a povinnostech.[468] Pověřenec je také zodpovědný za zodpovídání dotazů EIOÚ a spolupráci s ním, je-li to nutné. Podobně jako GDPR obsahuje nařízení (ES) č. 45/2001 ustanovení o nezávislosti pověřenců pro ochranu osobních údajů při plnění svých úkolu a nutnost jim poskytnout nezbytné zaměstnance a zdroje.[469] Pověřenci pro ochranu osobních údajů musí být zasláno oznámení, než daný orgán

467 Obecné nařízení o ochraně osobních údajů, čl. 38 odst. 2 a 3.

468 Viz čl. 24 odst. 1 nařízení (ES) č. 45/2001, kde lze najít úplný seznam úkolů pověřenců pro ochranu osobních údajů.

469 Nařízení (ES) č. 45/2001, čl. 24 odst. 6 a 7.

nebo instituce EU (nebo oddělení těchto organizací) provede jakékoliv operace zpracování, a musí vést rejstřík všech oznámených operací zpracování.[470]

4.3.2. Záznamy o činnostech zpracování

Společnosti mají často zákonnou povinnost vést dokumentaci a záznamy svých činností, aby byly schopny doložit dodržování právních předpisů a mohly nést zodpovědnost. Důležitým příkladem jsou daňové právní předpisy a audity, které vyžadují, aby všechny společnosti vedly rozsáhlou dokumentaci a záznamy. Stanovení podobných požadavků v jiných oblastech práva, zejména práva na ochranu osobních údajů, je také důležité, protože vedení záznamů je důležitým způsobem pro usnadňování dodržování pravidel v oblasti ochrany údajů. **Právo EU** tudíž stanoví, že správci nebo jejich zástupci musí vést záznam o činnostech zpracování, za něž odpovídají.[471] Tato povinnost má zajistit, že budou mít dozorové úřady v případě, že je to nutné, nezbytnou dokumentaci, která jim umožní potvrdit zákonnost zpracování.

K informacím, o nichž je třeba vést dokumentaci, patří:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,
- účely zpracování,
- popis kategorií subjektů údajů a kategorií osobních údajů souvisejících se zpracováním,
- informace o kategoriích příjemců, kterým byly nebo budou osobní údaje zpřístupněny,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci v minulosti či v budoucnosti,
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů, jakož i přehled technických a organizačních bezpečnostních opatření přijatých k zajištění bezpečnosti zpracování.[472]

470 Tamtéž, článek 25 a 26.

471 Obecné nařízení o ochraně osobních údajů, článek 30.

472 Tamtéž, čl. 30 odst. 1.

Povinnost vést záznamy o činnostech zpracování podle GDPR se týká nejen správců, ale i zpracovatelů. To je významná změna, protože před přijetím tohoto nařízení upravovala povinnosti zpracovatele primárně smlouva uzavřená mezi ním a správcem. Povinnost vést záznamy je nyní stanovena přímo v právních předpisech.

GDPR stanoví výjimku z této povinnosti. Povinnost vést záznamy se nepoužije v případě podniku nebo organizace (správce nebo zpracovatele), který zaměstnává méně než 250 osob. Tato výjimka však podléhá požadavku, aby dotčená organizace neprováděla zpracování, které pravděpodobně nepředstavuje riziko pro práva a svobody subjektů údajů, aby zpracování bylo pouze příležitostné a aby nezahrnovalo zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

Vedení záznamů o činnostech zpracování by mělo správcům a zpracovatelům umožnit prokázat soulad s nařízením. Mělo by také umožnit dozorovým úřadům monitorovat zákonnost zpracování. Pokud dozorové úřady požádají o přístup k těmto záznamům, jsou správci a zpracovatelé povinni spolupracovat a tyto záznamy dát k dispozici.

4.3.3. Posouzení vlivu na ochranu osobních údajů a předchozí konzultace

Operace zpracování představují určitá inherentní rizika pro práva jednotlivců. Osobní údaje mohou být ztraceny, sděleny neoprávněným stranám nebo zpracovány protiprávně. Rizika se přirozeně liší v závislosti na povaze a rozsahu zpracování. Rozsáhlé operace zpracování zahrnující zpracování citlivých údajů s sebou nesou například mnohem větší míru rizika pro subjekty údajů ve srovnání s možnými riziky, kdy malá společnost zpracovává adresy a osobní telefonní čísla svých zaměstnanců.

S nástupem nových technologií a s tím, jak se zpracování stává stále složitějším, musí se správci těmito riziky zabývat tím, že přezkoumají pravděpodobný dopad zamýšleného zpracování před zahájením operace zpracování. To umožňuje organizacím náležitě a předem identifikovat rizika, zabývat se jimi a zmírnit je, čímž se významně omezí pravděpodobnost nepříznivého dopadu na jednotlivce v důsledku zpracování.

Posouzení vlivu na ochranu údajů stanoví **právo RE i EU**. V právním rámci RE ukládá čl. 10 odst. 2 Modernizované úmluvy č. 108 smluvním stranám povinnost zajistit,

aby správci a zpracovatelé „prověřili pravděpodobný vliv zamýšleného zpracování údajů na práva a základní svobody subjektů údajů ještě před tím, než takové zpracování zahájí“, a po provedení posouzení navrhnout zpracování takovým způsobem, aby se zabránilo rizikům spojeným se zpracováním nebo aby se tato rizika minimalizovala.

Právo EU ukládá podobnou, podrobnější povinnost správcům spadajícím do působnosti GDPR. Článek 35 stanoví, že je třeba provést posouzení vlivu, pokud zpracování bude mít pravděpodobně za následek vysoké riziko pro práva a svobody jednotlivců. Nařízení nedefinuje, jak se má posuzovat pravděpodobnost rizika, ale naopak uvádí, co by mohlo tato rizika představovat.[473] Obsahuje seznam operací zpracování považovaných za vysoce rizikové, u nichž je předchozí posouzení vlivu zvlášť nezbytné, zejména v případech, kdy:

- se zpracovávají osobní údaje za účelem přijetí rozhodnutí o fyzických osobách v návaznosti na jakékoliv systematické a rozsáhlé hodnocení osobních aspektů týkajících se jednotlivců (profilování),

- se ve velkém měřítku zpracovávají citlivé údaje nebo osobní údaje týkající se odsouzení za trestný čin a trestných činů,

- zpracování zahrnuje monitorování veřejně přístupných prostor prováděné ve velkém rozsahu.

Dozorové úřady musí přijmout a zveřejnit seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu. Mohou rovněž vypracovat seznam operací zpracování vyňatých z této povinnosti.[474]

Vyžaduje-li se posouzení vlivu, musí správci posoudit nezbytnost a přiměřenost zpracování a možná rizika hrozící právům jednotlivců. Posouzení vlivu musí také obsahovat plánovaná bezpečnostní opatření, která se budou zabývat zjištěnými riziky. Dozorové úřady členských států jsou povinny spolupracovat na sestavení seznamů mezi sebou navzájem a s Evropským sborem pro ochranu osobních údajů. Tím se zajistí soudržný přístup v celé EU k operacím, které vyžadují posouzení vlivu, a správci budou vystaveni podobným požadavkům bez ohledu na to, kde se nacházejí.

473 Obecné nařízení o ochraně osobních údajů, preambule, 75. bod odůvodnění.

474 Tamtéž, čl. 35 odst. 4 a 5.

Pokud se po provedení posouzení vlivu zdá, že zpracování bude mít za následek vysoké riziko pro práva jednotlivců, a nebyla přijata žádná opatření na zmírnění rizika, musí správce konzultovat s příslušným dozorovým úřadem před zahájením operace zpracování.[475]

Pracovní skupina zřízená podle článku 29 vydala pokyny pro posouzení vlivu na ochranu údajů a pro to, jak posoudit, zda je pravděpodobné, že zpracování bude mít za následek vysoké riziko.[476] Vypracovala devět kritérií, která mají pomoci určit, zda posouzení vlivu na ochranu osobních údajů je v daném případě nutné:[477] 1) hodnocení nebo bodování, 2) automatizované rozhodování, které má právní nebo podobně závažný dopad, 3) systematické monitorování, 4) citlivé údaje, 5) údaje zpracovávané ve velkém rozsahu, 6) přiřazování nebo slučování datových souborů, 7) údaje týkající se zranitelných subjektů údajů, 8) nové použití nebo využití nových technologických nebo organizačních řešení, 9) pokud samotné zpracování „brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy". Pracovní skupina zřízená podle článku 29 zavedla orientační pravidlo, že zpracování, které splňuje méně než dvě kritéria, představuje nižší úroveň rizika a nevyžaduje posouzení z hlediska ochrany údajů, zatímco zpracování, jež splňují dvě a více kritérií, takovéto posouzení vyžadují. V případech, kdy není jasné, zda je posouzení vlivu na ochranu údajů vyžadováno, doporučuje pracovní skupina zřízená podle článku 29 toto posouzení provést, protože se jedná o „užitečný nástroj, který pomůže správcům zajistit soulad s právními předpisy v oblasti ochrany údajů".[478] Pokud se zavádí nová technologie zpracování údajů, je důležité, aby bylo provedeno posouzení vlivu na ochranu údajů.[479]

4.3.4. Kodexy chování

Kodexy chování mají být používány v několika průmyslových odvětvích s cílem nastínit a upřesnit uplatňování GDPR v daných odvětvích. Pro správce a zpracovatele osobních údajů může vytváření těchto kodexů značně zlepšit soulad s předpisy EU v oblasti ochrany údajů a posílit jejich provádění. Odborné znalosti členů odvětví

475 Tamtéž, čl. 36 odst.1; Pracovní skupina zřízená podle článku 29 (2017), *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, WP 248 rev.01, Brusel, 4. října 2017.

476 Pracovní skupina zřízená podle článku 29 (2017), *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*, WP 248 rev.01, Brusel, 4. října 2017.

477 Tamtéž, články 9–11.

478 Tamtéž, s. 9.

479 Tamtéž.

napomáhají nalézat řešení, která jsou praktická, a tudíž budou pravděpodobně následována. Nařízení GDPR uznává význam těchto kodexů pro účinné uplatňování práva v oblasti ochrany údajů a vyzývá členské státy, dozorové úřady, Komisi a Evropský sbor pro ochranu osobních údajů, aby podporovaly vypracování kodexů chování, které mají přispět k řádnému uplatňování tohoto nařízení v celé EU.[480] Kodexy by měly upřesňovat uplatňování tohoto nařízení v konkrétních odvětvích, včetně záležitostí, jako je shromažďování osobních údajů, informace poskytované subjektům údajů a veřejnosti a výkon práv subjektů údajů.

K zajištění, že kodexy chování jsou v souladu s pravidly stanovenými v GDPR, musí být kodexy před přijetím předloženy příslušnému dozorovému úřadu. Dozorový úřad pak vydá stanovisko k tomu, zda je daný návrh kodexu v souladu s tímto nařízením, a pokud shledá, že tento kodex poskytuje vhodné záruky, schválí jej.[481] Dozorové úřady musí zveřejnit schválený kodex chování i kritéria, na nichž je schválení založeno. Pokud se návrh kodexu chování týká činností zpracování v několika členských státech, příslušný dozorový úřad před schválením návrh kodexu či návrh na úpravu či rozšíření kodexu předloží Evropskému sboru pro ochranu osobních údajů, který vydá stanovisko k souladu kodexu s GDPR. Komise může prostřednictvím prováděcích aktů rozhodnout, že schválený kodex chování, který jí byl předložen, má všeobecnou platnost v rámci Unie.

Dodržování kodexu chování skýtá významné výhody pro subjekty údajů i pro správce a zpracovatele. Tyto kodexy poskytují podrobné pokyny, které upravují právní požadavky na míru konkrétním odvětvím a posilují transparentnost činností zpracování. Správci a zpracovatelé mohou také použít dodržování kodexů jako prokazatelný důkaz, že jednají v souladu s právem EU, a jako prostředek, jak zlepšit svůj veřejný obraz jako organizací, které přikládají vysokou prioritou ochraně osobních údajů při svých činnostech a zavazují se k této ochraně. Schválené kodexy chování spolu se závaznými a vymahatelnými závazky mohou být použity jako vhodné záruky pro předávání údajů do třetích zemí. K zajištění, že organizace, které mají kodexy chování, se jimi skutečně řídí, je možné jmenovat zvláštní subjekt (akreditovaný příslušným dozorovým úřadem) za účelem sledování a zajištění dodržování předpisů. Aby mohl tento subjekt účinně plnit své úkoly, musí být nezávislý, prokázat odborné znalosti v oblasti upravené kodexem chování a mít transparentní postupy a struktury pro řešení stížností na porušování kodexu.[482]

480 Obecné nařízení o ochraně osobních údajů, čl. 40 odst. 1.

481 Tamtéž, čl. 40 odst. 5.

482 Tamtéž, čl. 41 odst. 1 a 2.

V rámci **práva RE** stanoví Modernizovaná úmluva č. 108, že úroveň ochrany údajů zaručená vnitrostátním právem může být užitečným způsobem prosazována dobrovolnými regulačními nařízení, jako jsou kodexy osvědčených postupů nebo kodexy profesionálního chování. Podle Modernizované úmluvy č. 108 se však jedná pouze o dobrovolná opatření: není možné vyvodit žádnou právní povinnost zavádět tato opatření, ačkoliv jsou doporučena, a tato opatření sama o sobě nestačí k zajištění plného souladu s úmluvou.[483]

4.3.5. Vydávání osvědčení

Kromě kodexů chování jsou dalším prostředkem, který mohou správci a zpracovatelé použít k prokázání souladu s GDPR, mechanismy pro vydávání osvědčení, pečeti a známky. Proto nařízení stanoví dobrovolný systém vydávání osvědčení, v jehož rámci mohou vydávat osvědčení některé subjekty nebo dozorové úřady. Správci a zpracovatelé, kteří se rozhodnou řídit se mechanismem vydávání osvědčení, mohou získat větší publicitu a důvěryhodnost, protože osvědčení, pečeti a známky umožňují subjektům údajů rychle posoudit míru ochrany v oblasti zpracování údajů v dané organizaci. Je důležité připomenout, že skutečnost, že správce nebo zpracovatel vlastní toto osvědčení, nesnižuje jeho povinnosti a odpovědnost za dodržování všech požadavků právních předpisů.

4.4. Záměrná a standardní ochrana osobních údajů

Záměrná ochrana osobních údajů

Právo EU ukládá povinnost, aby správci zavedli opatření k účinnému provádění zásad ochrany údajů a začlenili do zpracování nezbytné záruky, tak aby splnili požadavky nařízení a ochránili práva subjektů údajů.[484] Tato opatření by měla být prováděna jak v době zpracování, tak při určování prostředků pro zpracování. Při provádění těchto opatření musí správci zohlednit soudobý stav, náklady provádění,

483 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 33.

484 Obecné nařízení o ochraně osobních údajů, čl. 25 odst. 1.

povahu, rozsah a účely zpracování osobních údajů a rizika a závažnost pro práva a svobody subjektu údajů.[485]

Právo RE ukládá povinnost, aby správci a zpracovatelé posuzovali pravděpodobný důsledek zpracování osobních údajů pro práva a svobody subjektů údajů před zahájením zpracování. Kromě toho jsou správci a zpracovatelé povinni navrhnout zpracování údajů tak, aby zabránili riziku zásahu do těchto práv a svobod nebo je minimalizovali, a provádět technická a organizační opatření, která zohledňují důsledky práva na ochranu osobních údajů ve všech fázích zpracování údajů.[486]

Standardní ochrana osobních údajů

Právo EU stanoví, že správci musejí provádět vhodná opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou nezbytné pro dané účely. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti.[487] Toto opatření musí například zajistit, aby neměli přístup k osobním údajům všichni zaměstnanci správců. Další pokyny byly vypracovány EIOÚ v dokumentu *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*.[488]

Právo RE stanoví povinnost, aby správci a zpracovatelé prováděli technická a organizační opatření k zohlednění důsledků práva na ochranu údajů a provedli technická a organizační opatření, která zohlední důsledky práva na ochranu osobních údajů ve všech fázích zpracování údajů.[489]

485 Viz pracovní skupina zřízená podle článku 29 (2017), Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679, WP 248 rev.01, 4. října 2017. Viz také ENISA (2015), Privacy and Data Protection by Design-from policy to engineering [Záměrná a standardní ochrana údajů – od politiky k realizaci], 12. ledna 2015.

486 Modernizovaná úmluva č. 108, čl. 10 odst. 2 a 3, Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 89.

487 Obecné nařízení o ochraně osobních údajů, čl. 25 odst. 2.

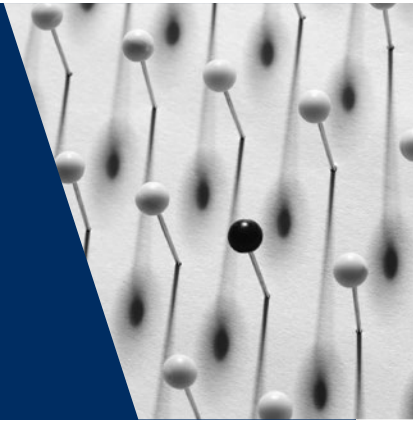
488 Evropský inspektor ochrany údajů (EIOÚ), (2017), *Necessity Toolkit [Soubor nástrojů na posouzení nezbytnosti]*, Brusel, 11. dubna 2017.

489 Modernizovaná úmluva č. 108, čl. 10 odst. 3, Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 89.

V roce 2016 agentura ENISA zveřejnila zprávu o dostupných nástrojích a službách v oblasti ochrany soukromí.[490] Kromě jiných aspektů toto posouzení stanoví rejstřík kritérií a parametrů, které jsou ukazateli dobrých a špatných postupů v oblasti ochrany soukromí. Zatímco některá kritéria se týkají přímo ustanovení GDPR – například používání pseudonymizace a schválených mechanismů vydávání osvědčení –, jiná stanoví inovativní iniciativy k zajištění ochrany soukromí již od návrhu (by design) a standardního nastavení ochrany soukromí (by default). Například kritérium použitelnosti, ačkoliv přímo nesouvisí se soukromím, může zvýšit ochranu soukromí, protože může umožnit širší přijetí nástroje nebo služby v oblasti ochrany soukromí. Nástroje v oblasti ochrany soukromí, které se obtížně zavádějí do praxe, může široká veřejnost zavádět skutečně jen ve velmi omezení míře, a to i když nabízejí velmi silné záruky v oblasti ochrany soukromí. Dále má klíčový význam kritérium vyzrálosti a stability nástroje v oblasti ochrany soukromí – čímž se rozumí způsob, jímž se nástroje v průběhu doby vyvíjí a reagují na stávající nebo nové výzvy související s ochranou soukromí. Jiné technologie posilující ochranu soukromí, například v souvislosti se zabezpečenými komunikacemi, obsahují šifrování mezi koncovými body (komunikace, kdy jedinými lidmi, kteří mohou číst zprávy, jsou ti, kteří spolu komunikují), šifrování klient-server (šifrování komunikačního kanálu vytvořeného mezi klientem a serverem), autentizace (ověřování totožnosti stran komunikace) a anonymní komunikace (žádná třetí strana nemůže identifikovat komunikující strany).

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools [Kontrolní matice pro technologie posilující ochranu soukromí: systematický přístup k posuzování on-line a mobilních nástrojů na ochranu soukromí], 20 prosince 2016.

5 Nezávislý dozor



EU	Pojednávaná témata	RE
Listina, čl. 8 odst. 3 Smlouva o fungování EU, čl. 16 odst. 2 Obecné nařízení o ochraně osobních údajů, články 51–59 Rozsudek SDEU (velkého senátu) z roku 2010, C-518/07, *Evropská komise v. Spolková republika Německo* Rozsudek SDEU (velkého senátu) z roku 2012, C-614/10, *Evropská komise v. Rakouská republika* Rozsudek SDEU (velkého senátu) z roku 2014, C-288/12, *Evropská komise v. Maďarsko* Rozsudek SDEU (velkého senátu) z roku 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*	**Dozorové úřady**	Modernizovaná úmluva č. 108, článek 15
Obecné nařízení o ochraně osobních údajů, články 60–67	**Spolupráce mezi dozorovými úřady**	Modernizovaná úmluva č. 108, články 16–21
Obecné nařízení o ochraně osobních údajů, články 68–76	**Evropský sbor pro ochranu osobních údajů**	

Hlavní body

- Nezávislý dozor je nezbytnou složkou evropského práva v oblasti ochrany údajů a je zakotven v čl. 8 odst. 3 Listiny.
- Aby byla zajištěna účinná ochrana údaje, musejí být podle vnitrostátního práva zřízeny nezávislé dozorové úřady.
- Dozorové úřady musí jednat zcela nezávisle a jejich nezávislost musí být zaručena zřizovacím právním předpisem a musí jí být přizpůsobena zvláštní organizační struktura dozorového úřadu.
- Dozorové úřady mají zvláštní pravomoci a povinnosti. Patří k nim mimo jiné:
  - sledovat a prosazovat ochranu údajů na vnitrostátní úrovni,
  - poskytovat poradenství subjektům údajů a správcům, ale také veřejné správě a veřejnosti obecně,
  - vyslechnout stížnosti a pomoci subjektům údajů v případech údajného porušení práv v oblasti ochrany údajů,
  - vykonávat dozor nad správci a zpracovateli.
- Dozorové úřady také mají pravomoc zasahovat, je-li to nutné, prostřednictvím:
  - varování, napomenutí, nebo dokonce udělení pokut správcům a zpracovatelům,
  - nařízení, aby byly údaje opraveny, zablokovány nebo vymazány,
  - uložení zákazu zpracování nebo správní pokuty,
  - postoupení věcí soudu.
- Jelikož zpracování osobních údajů často zahrnuje správce, zpracovatele a subjekty údajů nacházející se v různých státech, jsou dozorové úřady povinny spolupracovat mezi sebou navzájem v případě přeshraničních otázek za účelem účinné ochrany jednotlivců v Evropě.
- V EU obecné nařízení o ochraně osobních údajů stanoví mechanismus jediného kontaktního místa pro případy přeshraničního zpracovávání. Některé společnosti provádějí činnosti přeshraničního zpracování kvůli zpracovávání osobních údajů v souvislosti s činnostmi provozoven ve více než jednom členském státě nebo v souvislosti s jedinou provozovnou v Unii, která však významně ovlivňuje subjekty údajů ve více než jednom členském státě. V rámci tohoto mechanismu musejí tyto společnosti jednat pouze s jedním vnitrostátním dozorovým úřadem v oblasti ochrany údajů.

- Mechanismus spolupráce a jednotnosti umožní koordinovaný přístup mezi všemi dozorovými úřady zapojenými do dané věci. Vedoucí dozorový úřad – hlavní nebo jediné provozovny – bude konzultovat s ostatními dotčenými dozorovými úřady a předkládat jim návrh rozhodnutí.
- Podobně jako v případě současné pracovní skupiny zřízené podle článku 29 bude dozorový úřad každého členského státu a evropský inspektor ochrany údajů (EIOÚ) součástí Evropského sboru pro ochranu osobních údajů.
- K úkolům Evropského sboru pro ochranu osobních údajů patří například monitorování řádného uplatňování nařízení, poskytování poradenství Komisi v relevantních záležitostech a vydávání stanovisek, pokynů či osvědčených postupů na různá témata.
- Hlavní rozdíl je, že Evropský sbor pro ochranu osobních údajů nebude jen vydávat stanoviska, jak stanoví směrnice 95/46/ES. Bude také vydávat závazná rozhodnutí týkající se věcí, kdy některý dozorový úřad vznesl relevantní a odůvodněnou námitku v případech jediného kontaktního místa, kdy existují protichůdné názory na to, který dozorový úřad je vedoucí, a v neposlední řadě kdy příslušný dozorový úřad nepožádá o stanovisko Evropský sbor pro ochranu osobních údajů nebo se tímto stanoviskem neřídí. Cílem je zajistit soudržné uplatňování nařízení ve všech členských státech.

Nezávislý dozor je nezbytnou složkou evropského práva v oblasti ochrany údajů. Právo EU i RE nahlížejí na existenci nezávislých dozorových úřadů jako na nedílnou součást účinné ochrany práv a svobod jednotlivců, pokud jde o zpracování jejich osobních údajů. Jelikož je nyní zpracování údajů všudypřítomné a pro jednotlivce je stále složitější mu porozumět, jsou tyto úřady hlídacími psy digitálního věku. V EU se existence nezávislých dozorových úřadů považuje za jeden z nejzásadnějších prvků práva na ochranu osobních údajů, které je zakotveno v primárním právu EU. Článek 8 odst. 3 Listiny základních práv EU a čl. 16 odst. 2 SFEU uznávají, že ochrana osobních údajů je základním právem, a stvrzují, že soulad s pravidly v oblasti ochrany údajů musí podléhat kontrole ze strany nezávislého orgánu.

Význam nezávislého dozoru pro právo v oblasti ochrany údajů byl uznán i v judikatuře.

Příklad: Ve věci *Schrems*[491] měl SDEU obavy ohledně toho, zda předložení osobních údajů Spojeným státům americkým (USA) podle první dohody mezi EU a USA o „bezpečném přístavu" bylo v souladu s právem EU v oblasti ochrany údajů s ohledem na odhalení Edwarda Snowdena o tom, že agentura USA National Security Agency provádí hromadné sledování. Předávání

491 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

osobních údajů do USA bylo založeno na rozhodnutí Evropské komise přijatém v roce 2000, které umožňovalo předávání osobních údajů z EU organizacím v USA, které disponují vlastním osvědčením v rámci režimu „bezpečného přístavu", na základě toho, že režim zajišťuje odpovídající úroveň ochrany osobních údajů. Žadatel požádal o vyšetření stížnosti ohledně zákonnosti předávání údajů poté, co Snowden učinil svá odhalení. Irský dozorový úřad však stížnost zamítl z toho důvodu, že existence rozhodnutí Komise o odpovídající ochraně v rámci režimu USA pro ochranu údajů, která se odráží v zásadách „bezpečného přístavu" („rozhodnutí o bezpečném přístavu"), brání dalšímu vyšetřování stížnosti.

SDEU však rozhodl, že existence rozhodnutí Komise umožňujícího předávání údajů do třetích zemí, jež zaručují odpovídající úroveň ochrany, nepopírá ani neomezuje pravomoci vnitrostátních dozorových úřadů. SDEU konstatoval, že pravomoci těchto úřadů sledovat a zajišťovat dodržování pravidel EU v oblasti ochrany údajů vyplývají z primárního práva EU, zejména čl. 8 odst. 3 Listiny a čl. 16 odst. 2 SFEU. „Zřízení nezávislých orgánů dozoru v členských státech tedy představuje [...] zásadní prvek ochrany osob v souvislosti se zpracováním osobních údajů."[492]

SDEU proto rozhodl, že i když se předávání osobních údajů řídilo rozhodnutím Komise o odpovídající ochraně, pokud je vnitrostátnímu dozorovému úřadu předložena stížnost, musí ji tento úřad náležitě přezkoumat. Dozorový úřad může stížnost zamítnout, pokud shledá, že je neodůvodněná. V takovém případě SDEU zdůraznil, že právo na účinnou právní ochranu vyžaduje, aby jednotlivci měli možnost napadnout toto rozhodnutí u vnitrostátních soudů, které mohou věc postoupit SDEU formou žádosti o rozhodnutí o předběžné otázce týkající se platnosti rozhodnutí Komise. Pokud dozorový úřad považuje stížnost za odůvodněnou, musí být schopen zahájit právní řízení a předložit věc vnitrostátním soudům. Vnitrostátní soudy mohou věc postoupit SDEU, protože je to jediný subjekt, který má pravomoc rozhodnout o platnosti rozhodnutí Komise o odpovídající ochraně.[493]

492 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, bod 41.

493 Tamtéž, body 53–66.

SDEU následně přezkoumal platnost rozhodnutí o „bezpečném přístavu“, aby zjistil, zda systém předávání byl v souladu s pravidly EU v oblasti ochrany údajů. Zjistil, že článek 3 rozhodnutí o „bezpečném přístavu“ omezoval pravomoci vnitrostátních dozorových úřadů (udělené podle směrnice o ochraně údajů) přijmout opatření k zabránění předávání údajů v případě neodpovídající úrovně ochrany osobních údajů v USA. Vzhledem k významu nezávislých dozorových úřadů při zajišťování dodržování souladu s právními předpisy SDEU rozhodl, že podle směrnice o ochraně údajů a ve spojení s ustanoveními Listiny neměla Komise pravomoc omezit v tomto smyslu pravomoci nezávislých dozorových úřadů. Omezení pravomocí dozorových úřadů bylo jedním z důvodů, proč SDEU vyhlásil rozhodnutí o „bezpečném přístavu“ za neplatné.

Evropské právo tudíž stanoví nezávislý dozor jako důležitý mechanismus k zajištění účinné ochrany údajů. Nezávislé dozorové úřady jsou prvním kontaktním místem pro subjekty údajů ve věcech týkajících se narušení soukromí.[494] Podle práva EU i RE je zřízení dozorových úřadů povinné. Oba právní rámce popisují úkoly a pravomoci těchto orgánů podobně jako GDPR. V zásadě by dozorové úřady proto měly fungovat stejně podle práva EU i práva RE.[495]

5.1. Nezávislost

Právo EU a **právo RE** ukládají každému dozorovému úřadu povinnost jednat při plnění svých úkolů a při výkonu svých pravomocí naprosto nezávisle.[496] Nezávislost dozorového úřadu a jeho členů, jakož i zaměstnanců na přímých a nepřímých vnějších vlivech je zásadní pro zaručení plné objektivity při rozhodování o záležitostech týkajících se ochrany údajů. Nejenže musí právo, z něhož vychází zřízení dozorového orgánu, obsahovat ustanovení výslovně zaručující nezávislost, také musí nezávislost vykazovat organizační struktura úřadu. V roce 2010 SDEU – vůbec poprvé – zkoumal míru, v níž jsou dozorové úřady v oblasti ochrany údajů povinny být nezávislými.[497] Příklady, na něž se zde upozorňuje, ilustrují, jak SDEU definuje pojem „úplná nezávislost“.

494 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. d).

495 Tamtéž, článek 51; Modernizovaná úmluva č. 108, článek 15.

496 Obecné nařízení o ochraně osobních údajů, čl. 52 odst. 1; Modernizovaná úmluva č. 108, čl. 15 odst. 5.

497 FRA (2010), *Fundamental rights: challenges and achievements in 2010 [Základní práva: výzvy a úspěchy v roce 2010]*, Výroční zpráva za rok 2010, s. 59; FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities [Ochrana údajů v Evropské unii: úloha vnitrostátních úřadů na ochranu osobních údajů]*, květen 2010.

Příklad: Ve věci *Evropská komise v. Spolková republika Německo*[498] požádala Evropská komise SDEU, aby určil, že Německo nesprávně provedlo požadavek „úplné nezávislosti" orgánů pověřených zajistit ochranu údajů, a tudíž nesplnilo své povinnosti vyplývající z čl. 28 odst. 1 směrnice o ochraně údajů. Komise se domnívala, že skutečnost, že Německo zahájilo státní monitorování dozorových úřadů sledujících zpracování osobních údajů v jednotlivých spolkových zemích (*Länder*) s cílem zajistit soulad s právem v oblasti ochrany údajů, byla v rozporu s požadavkem nezávislosti.

SDEU zdůraznil, že slova „zcela nezávisle" je třeba vykládat na základě samotného znění tohoto ustanovení a na základě cílů a uspořádání práva EU v oblasti ochrany údajů.[499] SDEU zdůraznil, že dozorové úřady jsou „strážci" práv souvisejících se zpracováním osobních údajů. Jejich zřízení ve členských státech se tudíž pokládá za „zásadní prvek ochrany osob v souvislosti se zpracováním osobních údajů".[500] SDEU dospěl k závěru, že „při plnění svých úkolů musí orgány dozoru jednat objektivně a nestranně. Za tímto účelem musí být chráněny před jakýmkoli vnějším vlivem, včetně přímého či nepřímého vlivu státu."[501]

SDEU rovněž rozhodl, že význam spojení „úplná nezávislost" by měl být vykládán s ohledem na nezávislost EIOÚ, jak je vymezena v nařízení o ochraně údajů orgány EU. V tomto nařízení pojem nezávislosti vyžaduje, aby EIOÚ od nikoho nevyžadoval ani nepřijímal pokyny.

SDEU obdobně rozhodl, že dozorové úřady v Německu – kvůli dohledu orgánů veřejné moci – nebyly zcela nezávislé ve smyslu práva EU v oblasti ochrany údajů.

Příklad: Ve věci *Evropská komise v. Rakouská republika*[502] SDEU zdůraznil podobné problémy s nezávislostí některých členů a zaměstnanců rakouského orgánu pověřeného ochranou údajů (komise pro ochranu osobních údajů, DSK). SDEU dospěl k závěru, že skutečnost, že spolkové kancléřství

498 Rozsudek SDEU (velkého senátu) ze dne 9. března 2010, C-518/07, *Evropská komise v. Spolková republika Německo*, bod 27.

499 Tamtéž, body 17 a 29.

500 Tamtéž, bod 23.

501 Tamtéž, bod 25.

502 Rozsudek SDEU (velkého senátu) ze dne 16. října 2012, C-614/10, *Evropská komise v. Rakouská republika*, body 59 a 63.

poskytovalo dozorovému úřadu pracovníky, ohrožovala požadavek nezávislosti stanovený v právu EU v oblasti ochrany údajů. SDEU rovněž konstatoval, že požadavek vždy informovat kancléřství o své činnosti popíral úplnou nezávislost dozorového úřadu.

Příklad: Ve věci *Evropská komise v. Maďarsko*[503] byly zakázány podobné vnitrostátní praktiky ovlivňující nezávislost pracovníků. SDEU poukázal na to, že „požadavek […], podle něhož je třeba zaručit, že každý orgán kontroly plní úkoly, kterými je pověřen, zcela nezávisle, s sebou nese povinnost dotčeného členského státu respektovat délku mandátu takového orgánu, jak byla původně stanovena". SDEU rovněž rozhodl, že „Maďarsko tím, že předčasně ukončilo mandát orgánu dozoru na ochranu osobních údajů, nesplnilo povinnosti, které pro něj vyplývají ze směrnice 95/46/ES […]."

Pojem a kritéria „úplné nezávislosti" jsou nyní výslovně stanoveny v GDPR, které do sebe začleňuje zásady stanovené v popsaných rozsudcích SDEU. Podle nařízení zahrnuje úplná nezávislost při plnění jejich úkolů a výkonu jejich pravomocí tyto aspekty:[504]

- členové každého dozorového úřadu musí být i nadále nezávislí na vnějším vlivu – přímém či nepřímém – a od nikoho nesmějí vyžadovat ani přijímat pokyny,
- členové každého dozorového úřadu se musejí zdržet jakéhokoli jednání neslučitelného s jejich povinnostmi, aby zabránili střetu zájmů,
- členské státy musejí vybavit každý dozorový úřad lidskými, technickými a finančními zdroji a infrastrukturou pro účinné plnění jeho úkolů,
- členské státy zajistí, aby každý dozorový úřad vybíral své vlastní zaměstnance,
- finanční kontrola, které každý dozorový úřad podléhá podle vnitrostátního práva, nesmí ovlivnit jeho nezávislost. Dozorové úřady musí mít samostatný a veřejný roční rozpočet, který jim umožní náležité fungování.

503 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, C-288/12, *Evropská komise v. Maďarsko*, body 50 a 67.

504 Obecné nařízení o ochraně osobních údajů, článek 69.

Nezávislost dozorových úřadů se považuje za zásadní požadavek i podle práva RE. Modernizovaná úmluva č. 108 ukládá dozorovým úřadům povinnost jednat „při plnění svých povinností a výkonu pravomocí [...] zcela nezávisle a nestranně" a nevyhledávat ani nepřijímat pokyny.[505] Tím úmluva uznává, že tyto úřady nemohou účinně zaručit práva a svobody jednotlivců týkající se zpracování údajů, pokud nevykonávají své funkce zcela nezávisle. Vysvětlující zpráva k Modernizované úmluvě č. 108 stanoví řadu prvků, které přispívají k zabezpečení této nezávislosti. K těmto prvkům patří možnost, aby dozorové úřady najímaly vlastní zaměstnance a přijímaly rozhodnutí, aniž by byly vystaveny vnějšímu vlivu, jakož i faktory týkající se doby trvání výkonu jejich funkcí a podmínek, za nichž mohou výkon těchto funkcí ukončit.[506]

5.2. Příslušnost a pravomoci

Podle práva EU stanoví GDPR příslušnost a organizační strukturu dozorových úřadů a požaduje, aby byly příslušnými orgány a měly pravomoci plnit úkoly stanovené tímto nařízením.

Dozorový úřad je hlavním subjektem ve vnitrostátním právu, který zajišťuje soulad s právem EU v oblasti ochrany údajů. Dozorové úřady mají komplexní soubor úkolů a pravomocí nad rámec monitorování. K nim patří i proaktivní a preventivní činnosti v oblasti dohledu. K plnění těchto úkolů musí mít dozorové úřady vhodné vyšetřovací, nápravné a poradní pravomoci, které jsou vyjmenovány v článcích 57–58 GDPR, např.:[507]

- poskytovat poradenství správcům a subjektům údajů ve všech záležitostech týkajících se ochrany údajů,
- povolovat standardní smluvní doložky, závazná podniková pravidla nebo správní ujednání,
- vyšetřovat operace zpracování a náležitě zasáhnout,

505 Modernizovaná úmluva č. 108, čl. 15 odst. 5.

506 Vysvětlující zpráva k Modernizované úmluvě č. 108.

507 Obecné nařízení o ochraně osobních údajů, články 57–58. Viz též Úmluvu č. 108, Dodatkový protokol, článek 1.

- uložit povinnost předkládat veškeré informace relevantní pro dozor nad činnostmi správce,
- vydávat varování nebo udělovat napomenutí správcům a nařizovat zaslání oznámení případů porušení zabezpečení osobních údajů subjektům údajů,
- nařizovat opravu, blokování, výmaz nebo zničení údajů,
- uložit dočasný nebo trvalý zákaz zpracování nebo uložit správní pokuty,
- postoupit věc soudu.

K výkonu svých funkcí musí mít dozorový úřad přístup ke všem osobním údajům a informacím nezbytným pro dané šetření, jakož i přístup do veškerých prostor, kde správce uchovává relevantní informace. Podle SDEU musí být pravomoci dozorového úřadu vykládány široce, aby se zajistila plná účinnost ochrany údajů pro subjekty údajů v EU.

Příklad: Ve věci *Schrems* měl SDEU obavy ohledně toho, zda předávání osobních údajů do USA podle první dohody mezi EU a USA o „bezpečném přístavu" bylo v souladu s právem EU v oblasti ochrany údajů s ohledem na skutečnosti odhalené Edwardem Snowdenem. Odůvodnění SDEU znělo, že vnitrostátní dozorové úřady – vystupující ve své úloze nezávislých subjektů monitorování zpracování údajů správci – mohou zabránit předávání osobních údajů do třetí země navzdory existenci rozhodnutí o odpovídající ochraně, pokud existují rozumné důkazy, že v dané třetí zemi již není zaručena odpovídající ochrana.[508]

Každý dozorový úřad je příslušný k výkonu vyšetřovacích pravomocí a pravomocí zasahovat na svém území. Avšak činnosti správců a zpracovatelů jsou často přeshraniční povahy a zpracování údajů ovlivňuje subjekty údajů nacházející se ve více členských státech, a proto vyvstává otázka po rozdělení příslušnosti mezi jednotlivé dozorové úřady. SDEU měl příležitost tuto otázku přezkoumat ve věci *Weltimmo*.

508 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, body 26–36 a 40–41.

Příklad: Ve věci *Weltimmo*[509] se SDEU zabýval příslušností vnitrostátních dozorových úřadů, pokud jde o vyřizování záležitostí týkajících se organizací, které nebyly usazeny v jejich jurisdikci. Weltimmo je společnost se sídlem na Slovensku provozující webové stránky pro inzerci maďarských nemovitostí. Inzerenti podali stížnost k maďarskému orgánu dozoru na porušení maďarského zákona o ochraně údajů a orgán uložil společnosti pokutu. Společnost uložení pokuty napadla u vnitrostátních soudů a věc byla postoupena SDEU, aby rozhodl, zda směrnice EU o ochraně osobních údajů umožňovala dozorovým úřadům jednoho členského státu uplatňovat své vnitrostátní právní předpisy na ochranu údajů společnosti se sídlem v jiném členském státě.

SDEU vyložil čl. 4 odst. 1 písm. a) směrnice o ochraně údajů tak, že umožňuje uplatnění právních předpisů v oblasti ochrany údajů členského státu, který není členským státem, v němž je usazen správce, „za předpokladu, že tento správce vykonává prostřednictvím stálého zařízení na území tohoto členského státu efektivní a skutečnou činnost, byť i minimální, v rámci níž je prováděno toto zpracování". SDEU konstatoval, že na základě informací, které mu byly předloženy, společnost Weltimmo provozovala v Maďarsku efektivní a skutečnou činnost, protože společnost měla v Maďarsku zástupce zapsaného ve slovenském obchodním rejstříku s maďarskou adresou, dále měla maďarský bankovní účet a poštovní schránku a také vykonávala v Maďarsku činnosti napsané v maďarštině. Tyto informace svědčily o existenci provozovny a vedly by k tomu, že činnost společnosti Weltimmo se řídí maďarským právem na ochranu údajů a je v jurisdikci maďarského dozorového úřadu. SDEU však ponechal na vnitrostátním soudu, aby informace ověřil a rozhodl, zda skutečně měla společnost Weltimmo provozovnu v Maďarsku.

Pokud postupující soud shledal, že společnost Weltimmo má provozovnu v Maďarsku, bude mít maďarský dozorový úřad pravomoc uložit pokutu. Avšak pokud by vnitrostátní soud rozhodl opačně, tj. že společnost Weltimmo nemá provozovnu v Maďarsku, bylo by potom rozhodným právem právo členského státu (členských států), kde má společnost sídlo. V tomto případě, protože pravomoci dozorových úřadů musí být vykonávány v souladu s územní suverenitou jiných členských států, by maďarský orgán nemohl ukládat sankce. Jelikož však směrnice o ochraně údajů obsahovala povinnost

509 Rozsudek SDEU ze dne 1. října 2015, C-230/14, *Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*.

spolupráce dozorových úřadů, mohl maďarský orgán požádat svůj slovenský protějšek, aby záležitost přezkoumal, určil, zda bylo porušeno slovenské právo, a uložil sankce stanovené podle slovenské legislativy.

Po přijetí GDPR jsou nyní zavedena podrobná pravidla týkající se příslušnosti dozorových úřadů v přeshraničních věcech. Nařízením se zřizuje „mechanismus jediného kontaktního místa" a nařízení obsahuje ustanovení ukládající povinnost spolupráce mezi jednotlivými dozorovými úřady. Pro účinnou spolupráci v přeshraničních věcech ukládá GDPR povinnost určit vedoucí dozorový úřad, kterým bude dozorový úřad hlavní nebo jediné provozovny správce či zpracovatele.[510] Vedoucí dozorový úřad je pověřen přeshraničními věcmi, je jediným úřadem vstupujícím do styku se správcem či zpracovatelem a koordinuje spolupráce s jinými dozorovými úřady ve snaze dosáhnout konsenzu. Spolupráce zahrnuje výměnu informací, vzájemnou pomoc s monitorováním a vedením šetření a přijímání závazných rozhodnutí.[511]

Podle práva RE jsou příslušnost a pravomoci dozorových úřadů stanoveny v článku 15 Modernizované úmluvy č. 108. Tyto pravomoci odpovídají pravomocím dozorových úřadů podle práva EU, včetně pravomocí provádět vyšetřování a zásahy, pravomoci vydávat rozhodnutí a ukládat správní sankce za porušení ustanovení úmluvy a pravomocí zahájit právní řízení. Nezávislé dozorové úřady mají také pravomoc vyřizovat žádosti a stížnosti předložené subjekty údajů, zvyšovat povědomí veřejnosti o právu v oblasti ochrany údajů a poskytovat poradenství vnitrostátním rozhodujícím subjektům ohledně veškerých legislativních nebo správních opatření, která vyžadují zpracování osobních údajů.

5.3. Spolupráce

GDPR stanoví obecný rámec spolupráce mezi dozorovými úřady a konkrétnější pravidla spolupráce dozorových úřadů při přeshraničních činnostech zpracování osobních údajů.

Podle GDPR si musejí dozorové úřady poskytovat vzájemnou pomoc a sdílet relevantní informace za účelem soudržného provádění a uplatňování nařízení.[512] Součástí této povinnosti je i to, že dožádaný dozorový úřad musí provádět konzultace,

510 Obecné nařízení o ochraně osobních údajů, čl. 56 odst. 1.

511 Tamtéž, článek 60.

512 Tamtéž, čl. 61 odst. 1 až 3 a čl. 62 odst. 1.

inspekce a šetření. Dozorové úřady mohou provádět společné postupy, včetně společných šetření a společných donucovacích opatření, do nichž jsou zapojeni pracovníci všech dozorových úřadů.[513]

V EU správci a zpracovatelé stále častěji působí na nadnárodní úrovni. K tomu je zapotřebí úzká spolupráce mezi příslušnými dozorovými úřady v členských státech, která zajistí, že zpracování osobních údajů probíhá v souladu s požadavky GDPR. Mechanismus „jednotného kontaktního místa", stanovený nařízením, znamená, že pokud správce nebo zpracovatel má provozovny v několika členských státech nebo pokud má jedinou provozovnu, ale operacemi zpracování budou podstatně dotčeny subjekty údajů ve více než jednom členském státě, je vedoucím dozorovým úřadem pro přeshraniční činnosti správce nebo zpracovatele dozorový úřad hlavní (nebo jediné) provozovny. Vedoucí dozorové úřady mají pravomoc přijmout donucovací opatření proti správci nebo zpracovateli. Cílem mechanismu jednotného kontaktního místa je zlepšit harmonizaci a jednotné uplatňování práva EU v oblasti ochrany údajů v různých členských státech. Přináší výhody také pro podniky, protože se musí jednat pouze s vedoucím dozorovým úřadem, nikoliv s několika dozorovými úřady. Tím se zvyšuje právní jistota pro podniky a v praxi by to mělo znamenat, že rozhodnutí se přijímají rychleji a že podniky nečelí různým dozorovým úřadům, které jim ukládají rozporné povinnosti.

K určení vedoucího dozorového orgánu je třeba určit umístění hlavní provozovny daného podniku v EU. Pojem „hlavní provozovna" je definován v GDPR. Dále pak pracovní skupina zřízená podle článku 29 vydala pokyny k určení vedoucího dozorového úřadu daného správce nebo zpracovatele, jejichž součástí jsou kritéria pro určení hlavní provozovny. [514]

Má-li být zajištěna vysoká úroveň ochrany údajů v celé EU, nemůže vedoucí dozorový úřad jednat osamoceně. Musí spolupracovat s ostatními dotčenými dozorovými úřady s cílem přijímat rozhodnutí o zpracování osobních údajů ze strany správců a zpracovatelů ve snaze dosáhnout konsenzu a zajistit soudržnost. Spolupráce mezi příslušnými dozorovými úřady zahrnuje výměnu informace, vzájemnou pomoc, provádění společných šetření a činností sledování.[515] Při poskytování vzájemné pomoci musí dozorové úřady náležitě vyřizovat žádosti o informace předložené jinými

513 Tamtéž, čl. 62 odst. 1.

514 Pracovní skupina zřízená podle článku 29 (2016), *Pokyny pro určení vedoucího dozorového úřadu správce nebo zpracovatele*, WP 244, Brusel, 13. prosince 2016, revidováno dne 5. dubna 2017.

515 Obecné nařízení o ochraně osobních údajů, čl. 60 odst. 1–3.

dozorovými úřady a provádět dozorová opatření, jako je například předchozí povolení a konzultace se správcem údajů o jeho činnostech zpracování, inspekcích nebo šetřeních. Vzájemná pomoc dozorovým úřadům v jiných členských státech musí být poskytována na požádání neprodleně a nejpozději do jednoho měsíce od obdržení žádosti.[516]

Pokud má správce provozovny ve více členských státech, mohou dozorové úřady provádět společné postupy, včetně společných šetření a společných donucovacích opatření, do nichž jsou zapojeni pracovníci dozorových úřadů z jiných členských států.[517]

Spolupráce mezi jednotlivými dozorovými úřady je důležitým požadavkem i podle práva RE. Modernizovaná úmluva č. 108 stanoví, že dozorové úřady musejí vzájemně spolupracovat v rozsahu nezbytném k plnění jejich úkolů.[518] Toho lze dosáhnout například tím, že si budou navzájem poskytovat relevantní a užitečné informace a koordinovat šetření a provádění společných postupů.[519]

5.4. Evropský sbor pro ochranu osobních údajů

Význam nezávislých dozorových úřadů a hlavní pravomoci, které požívají podle evropského práva v oblasti ochrany údajů, byly popsány v předcházejících odstavcích této kapitoly. Evropský sbor pro ochranu osobních údajů (EDPB) je dalším významným subjektem při zajišťování, aby byla pravidla v oblasti ochrany údajů uplatňována účinně a soudržně v celé EU.

Nařízením GDPR se zřídil sbor EDPB jako orgán EU s právní subjektivitou.[520] Jedná se o nástupce pracovní skupiny zřízené podle článku 29[521], která byla zřízena podle

516 Tamtéž, čl. 61 odst. 1 a 2.

517 Tamtéž, čl. 62 odst. 1.

518 Modernizovaná úmluva č. 108, článek 16 a 17.

519 Tamtéž, čl. 17.

520 Obecné nařízení o ochraně osobních údajů, článek 68.

521 Směrnice 95/46/ES stanoví, že pracovní skupina zřízená podle článku 29 má poskytovat Komisi poradenství o všech opatřeních EU, která se týkají práv jednotlivců v souvislosti se zpracováním osobních údajů a soukromím, prosazovat jednotné uplatňování směrnice a poskytovat odborné stanovisko Komisi k záležitostem týkajícím se ochrany údajů. Pracovní skupina zřízená podle článku 29 se skládá ze zástupců dozorových orgánů členských států EU a také z Komise a EIOÚ.

směrnice o ochraně údajů za tím účelem, aby poskytovala poradenství Komisi ohledně veškerých opatření EU, která se týkají práv jednotlivců v souvislosti se zpracováním osobních údajů a soukromím, prosazovala jednotné uplatňování směrnice a poskytovala odborné stanovisko Komisi k záležitostem týkajícím se ochrany údajů. Pracovní skupina zřízená podle článku 29 se skládá ze zástupců dozorových orgánů členských států EU spolu se zástupci Komise a EIOÚ.

Sbor EDPB tvoří obdobně jako pracovní skupinu předsedové dozorových úřadů každého členského státu a EIOÚ nebo jejich zástupci.[522] EIOÚ má stejná hlasovací práva s výjimkou případů souvisejících s řešením sporů, kdy může hlasovat pouze o rozhodnutích týkajících se zásad a pravidel platných pro orgány EU, které obsahově odpovídají zásadám a pravidlům uvedeným v GDPR. Komise má právo účastnit se činností a schůzek EDPS, ale nemá hlasovací práva.[523] Sbor si z řad svých členů volí předsedu (který je pověřen zastupováním skupiny) a dva místopředsedy na pětileté funkční období prostou většinou hlasů. Kromě toho má EDPS k dispozici také sekretariát, který zajišťuje EIOÚ, aby měl sbor analytickou, administrativní a logistickou podporu.[524]

Úkoly EDPS jsou podrobně uvedeny v článcích 64, 65 a 70 GDPR a patří k nim komplexní povinnosti, které je možné rozdělit na tři hlavní činnosti:

- **Jednotnost:** EDPB může vydávat právně závazná rozhodnutí ve třech případech: pokud některý dozorový úřad vznesl relevantní a odůvodněnou námitku v případech jediného kontaktního místa, pokud existují protichůdné názory na to, který dozorový úřad je „vedoucí", a v neposlední řadě pokud příslušný dozorový úřad nepožádá o stanovisko EDPB nebo se tímto stanoviskem neřídí.[525] Hlavní povinností EDPB je zajistit, aby GDPR bylo důsledně uplatňováno v celé EU, a plní zásadní úlohu v rámci mechanismu jednotnosti, jak je popsáno v oddíle 5.5.

- **Konzultace:** K úkolům EDPB patří poskytování poradenství Komisi ohledně všech záležitostí, které souvisejí s ochranou osobních údajů v Unii, jako jsou změny GDPR, revize právních předpisů EU, které zahrnují zpracování údajů a mohly by být v rozporu s pravidly EU v oblasti ochrany údajů, nebo vydání rozhodnutí o odpovídající ochraně ze strany Komise, která umožňují předávání osobních údajů do třetí země nebo mezinárodní organizaci.

522 Obecné nařízení o ochraně osobních údajů, čl. 68 odst. 3.

523 Tamtéž, čl. 68 odst. 4 a 5.

524 Tamtéž, článek 73 a 75.

525 Tamtéž, článek 65.

- **Pokyny:** Sbor rovněž vydává pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování tohoto nařízení, a prosazuje spolupráci a výměnu znalostí mezi dozorovými úřady. Kromě toho musí podporovat sdružení správců nebo zpracovatelů při vypracovávání kodexů chování, jakož i při zavedení pečetí a známek dokládajících ochranu údajů.

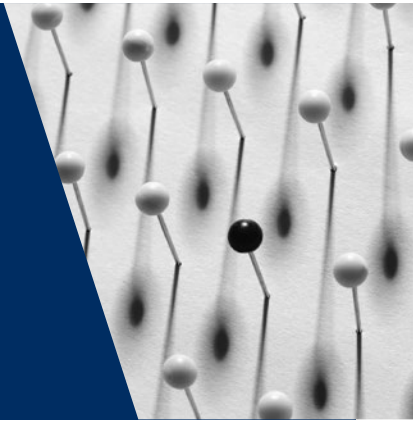
Rozhodnutí EDPB je možné napadnout u SDEU.

5.5. Mechanismus jednotnosti podle GDPR

GDPR zavádí mechanismus jednotnosti, který má zajistit, aby se nařízení uplatňovalo důsledně ve všech členských státech, přičemž prostřednictvím tohoto mechanismu vzájemně spolupracovaly dozorové úřady mezi sebou a případně s Komisí. Mechanismus jednotnosti se uplatní ve dvou situacích. První se týká stanovisek EDPB v případech, kdy příslušný dozorový úřad má v úmyslu přijmout opatření, jako je seznam operací zpracování, pro které je nutné posouzení vlivu na ochranu osobních údajů, nebo pokud má v úmyslu rozhodnout o standardních smluvních doložkách. Druhý se týká rozhodnutí EDPB, která jsou pro dozorové úřady závazná, v případech týkajících se jednotného kontaktního místa, a pokud dozorový úřad nepožádá o stanovisko EDPB nebo se jím neřídí.

6

Práva subjektů údajů a jejich vynucování



EU	Pojednávaná témata	RE
Právo být informován		
Obecné nařízení o ochraně osobních údajů, článek 12 Rozsudek SDEU z roku 2013, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert* Rozsudek SDEU z roku 2015, C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*	**Transparentnost informací**	Modernizovaná úmluva č. 108, článek 8
Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 1 a 2 a čl. 14 odst. 1 a 2	**Obsah informací**	Modernizovaná úmluva č. 108, čl. 8 odst. 1
Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 1 a čl. 14 odst. 3	**Doba poskytování informací**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. b).
Obecné nařízení o ochraně osobních údajů, čl. 12 odst. 1, 5 a 7	**Prostředky poskytování informací**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. b).
Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. d) a čl. 14 odst. 2 písm. e), články 77, 78 a 79	**Právo podat stížnost**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. f)

EU	Pojednávaná témata	RE
Právo na přístup k údajům		
Obecné nařízení o ochraně osobních údajů, čl. 15 odst. 1 Rozsudek SDEU z roku 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer* Rozsudek SDEU z roku 2014, spojené věci C-141/12 a C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M a S* Rozsudek SDEU (velkého senátu) z roku 2017, C-434/16, *Peter Nowak v. Data Protection Commissioner*	**Právo na přístup k vlastním údajům**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. b) Rozsudek ESLP z roku 1987, *Leander v. Švédsko*, č. 9248/81
Právo na opravu		
Obecné nařízení o ochraně osobních údajů, článek 16	**Oprava nepřesných osobních údajů**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. e) Rozsudek ESLP z roku 2008, *Cemalettin Canli v. Turecko*, č. 22427/04 Rozsudek ESLP z roku 2010, *Ciubotaru v. Moldavsko*, č. 27138/04
Právo na výmaz		
Obecné nařízení o ochraně osobních údajů, čl. 17 odst. 1	**Výmaz osobních údajů**	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. e) Rozsudek ESLP z roku 2006, *Segerstedt-Wiberg a další v. Švédsko*, č. 62332/00
Rozsudek SDEU (velkého senátu) z roku 2014, C-131/12, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González* Rozsudek SDEU z roku 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*	**Právo být zapomenut**	

EU	Pojednávaná témata	RE
Právo na omezení zpracování		
Obecné nařízení o ochraně osobních údajů, čl. 18 odst. 1	Právo na omezení používání osobních údajů	
Obecné nařízení o ochraně osobních údajů, článek 19	Oznamovací povinnost	
Právo na přenositelnost údajů		
Obecné nařízení o ochraně osobních údajů, článek 20	Právo na přenositelnost údajů	
Právo vznést námitku		
Obecné nařízení o ochraně osobních údajů, čl. 21 odst. 1 Rozsudek SDEU z roku 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*	Právo vznést námitku vzhledem ke konkrétní situaci subjektu údajů	Doporučení o profilování, článek 5.3 Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. d)
Obecné nařízení o ochraně osobních údajů, čl. 21 odst. 2	Právo vznést námitky ohledně použití údajů pro marketingové účely	Doporučení k přímému marketingu, článek 4.1
Obecné nařízení o ochraně osobních údajů, čl. 21 odst. 5	Právo vznést námitku automatizovanými prostředky	
Práva související s automatizovaným rozhodováním a profilováním		
Obecné nařízení o ochraně osobních údajů, článek 22	Práva související s automatizovaným rozhodováním a profilováním	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. a)
Obecné nařízení o ochraně osobních údajů, článek 21	Právo vznést námitku proti automatizovanému rozhodování	
Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. f)	Práva na smysluplné vysvětlení	Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. c)

EU	Pojednávaná témata	RE
Právní ochrana, odpovědnost, sankce a odškodnění		
Listina, článek 47 Rozsudek SDEU (velkého senátu) z roku 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* Obecné nařízení o ochraně osobních údajů, články 77–84	**V případě porušení vnitrostátního práva v oblasti ochrany údajů**	EÚLP, článek 13 (pouze pro členské státy RE) Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. f), články 12, 15, 16–21 Rozsudek ESLP z roku 2008, *K.U. v. Finsko*, č. 2872/02 Rozsudek ESLP ze dne 2008, *Biriuk v. Litva*, č. 23373/03
Nařízení o ochraně údajů orgány EU, články 34 a 49 Rozsudek SDEU (velkého senátu) z roku 2010, C-28/08 P, *Evropská komise v. The Bavarian Lager Co. Ltd*	**V případě porušení práva EU ze strany orgánů a institucí EU**	

Účinnost právních předpisů obecně a práv subjektů údajů zvlášť závisí do značné míry na existenci vhodných mechanismů k jejich vynucování. V digitálním věku se zpracování údajů stává všudypřítomným a pro jednotlivce je stále složitější je pochopit. Ke zmírnění nerovnováhy moci mezi subjekty údajů a správci získali jednotlivci určitá práva na provádění větší kontroly zpracování svých osobních informací. Právo na přístup k vlastním údajům a právo nechat údaje opravit jsou zakotvena v čl. 8 odst. 2 Listiny základních práv EU, což je dokument, který představuje primární právo EU a má zásadní hodnotu v právním řádu EU. Sekundární právo EU – zejména obecné nařízení o ochraně osobních údajů – stanoví soudržný právní rámec, který posiluje postavení subjektů údajů tím, že jim poskytuje práva týkající se správců údajů. Kromě práv na přístup a opravu uznává GDPR řadu dalších práv, jako je právo na výmaz („právo být zapomenut“), právo vznést námitku nebo omezit zpracování údajů, a práva související s automatizovaným rozhodováním a profilováním. Podobné záruky umožňující subjektům údajů vykonávat účinnou kontrolu nad svými údaji jsou obsaženy také v Modernizované úmluvě č. 108. V článku 9 se uvádí výčet práv, která by jednotlivci měli být schopni vykonávat, pokud jde o zpracování jejich osobních údajů. Smluvní strany musí zajistit, že tato práva jsou dostupná každému subjektu údajů v jejich jurisdikci a že jsou doplněna o účinné právní a praktické prostředky, které umožňují subjektům údajů jejich výkon.

Vedle poskytnutí práv jednotlivcům je stejně důležité zřídit mechanismy, které subjektům údajů umožní napadnout porušení jejich práv, zajistit odpovědnost správců

a požadovat odškodnění. Právo na účinnou právní ochranu, jak je zaručuje EÚLP a Listina, vyžaduje, aby byla soudní ochrana dostupná každé osobě.

6.1. Práva subjektů údajů

Hlavní body

- Každý subjekt údajů má kromě několika omezených výjimek právo na informace o veškerém zpracování svých osobních údajů ze strany správce údaje.
- Subjekty údajů mají právo:
  - získat přístup k vlastním údajům a obdržet určité informace o zpracování,
  - dosáhnout opravy svých údajů ze strany správce zpracovávajícího jejich údaje, jsou-li údaje nepřesné,
  - přimět správce případně vymazat jejich údaje, pokud správce jejich údaje zpracovává protiprávně,
  - dočasně omezit zpracování,
  - za určitých okolností nechat údaje přesunout k jinému správci.
- Kromě toho mají subjekty údajů právo vznést námitku proti zpracovávání:
  - na základě důvodů souvisejících s jejich konkrétní situací,
  - týkající se použití jejich údajů pro účely přímého marketingu.
- Subjekty údajů mají právo nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování, které mají právní účinky nebo které se subjektů významně dotýkají. Subjekty údajů také mají právo:
  - na lidský zásah ze strany správce,
  - vyjádřit svůj názor a napadnout rozhodnutí založené na automatizovaném zpracování.

6.1.1. Právo být informován

Podle **práva RE** i podle **práva EU** jsou správci operací zpracování povinni informovat subjekt údajů v okamžiku, kdy se shromažďují osobní údaje, o jejich zamýšleném zpracování. Tato povinnost nezávisí na tom, zda subjekt údajů předloží žádost, ale naopak – správce musí aktivně plnit tuto povinnost bez ohledu na to, zda subjekt údajů projeví zájem o tyto informace, či nikoliv.

Podle práva RE musí smluvní strany, jak je v uvedeno v článku 8 Modernizované úmluvy č. 108, stanovit, že správci musejí informovat subjekty údajů o své totožnosti a obvyklém místě pobytu, právním základu a účelu zpracování, kategoriích zpracovávaných osobních údajů, (případných) příjemcích jejich osobních údajů a o tom, jak mohou vykonávat svá práva podle článku 9, k nimž patří právo na přístup, opravu a právní ochranu. Subjektům údajů by také měly být sděleny veškeré další informace považované za nezbytné k zajištění spravedlivého a transparentního zpracování osobních údajů. Vysvětlující zpráva k Modernizované úmluvě č. 108 objasňuje, že informace předkládané subjektům údajů „by měly být snadno přístupné, čitelné, srozumitelné a přizpůsobené příslušným subjektům údajů".[526]

Podle práva EU stanoví zásada transparentnosti povinnost, aby zpracování osobních údajů bylo obecně vzato pro jednotlivce transparentní. Jednotlivci mají právo dozvědět se, jak a jaké osobní údaje se shromažďují, používají nebo jinak zpracovávají, ale také by měli být upozorněni na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním.[527] Článek 12 GDPR tudíž stanoví širokou, komplexní povinnost správců poskytovat transparentní informace a/nebo sdělovat, jak mohou subjekty údajů vykonávat svá práva.[528] Informace musí být stručné, transparentní, srozumitelné a snadno přístupné a musejí používat jasných a jednoduchých jazykových prostředků. Musí být poskytnuty písemně, mimo jiné ve vhodných případech elektronicky, a mohou být dokonce poskytnuty ústně na žádost subjektu údajů, a pokud je identita subjektu údajů prokázána nade vši pochybnost. Informace se poskytují bez zbytečného odkladu či nákladů.[529]

Články 13 a 14 GDPR se zabývají právem subjektů údajů být informováni, ať už v situaci, kdy byly osobní údaje shromážděny přímo od nich (článek 13), nebo v situacích, kdy údaje od nich získány nebyly (článek 14).

Působnost práva na informace a jeho omezení podle práva EU byly objasněny v judikatuře SDEU.

526 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 68.

527 Obecné nařízení o ochraně osobních údajů, 39. bod odůvodnění.

528 Tamtéž, článek 13 a 14; Modernizovaná úmluva č. 108, čl. 8 odst. 1 písm. b).

529 Obecné nařízení o ochraně osobních údajů, čl. 12 odst. 5, Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. b).

Příklad: Ve věci *Institut professionnel des agents immobiliers (IPI) v. Englebert*[530] byl SDEU požádán, aby vyložil čl. 13 odst. 1 směrnice 95/46/ES. Tento článek dával členským státům na výběr, zda přijmou legislativní opatření s cílem omezit rozsah práv subjektů údajů na to, být informován, je-li to nezbytné k ochraně mimo jiné práv a svobod druhých nebo k předcházení trestným činům a jejich vyšetřování nebo nedodržování deontologických pravidel pro regulovaná povolání. IPI je profesní organizace realitních makléřů v Belgii, která je odpovědná za zajištění souladu s náležitým výkonem povolání realitního makléře. Tato organizace požádala vnitrostátní soud, aby prohlásil, že žalovaní porušili profesní pravidla, a nařídil jim, aby ukončili různé činnosti realitní kanceláře. Žaloba byla založena na důkazech poskytnutých soukromými detektivy, které si najala organizace IPI.

Vnitrostátní soud měl pochybnosti o hodnotě důkazů detektivů vzhledem k možnosti, že byly získány v rozporu s požadavky na ochranu údajů stanovenými v belgickém právním řádu, zejména povinností informovat subjekty údajů o zpracování jejich osobních údajů před zahájením shromažďování informací. SDEU konstatoval, že v čl. 13 odst. 1 se uvádí, že členské státy „mohou", ale nemají povinnost zavést do svého vnitrostátního práva výjimky z povinnosti informovat subjekty údajů o zpracování jejich údajů. Jelikož čl. 13 odst. 1 zahrnuje předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo nedodržování deontologických pravidel jako důvody, pro které mohou členské státy omezit práva jednotlivců, činnost subjektu, jako je IPI, a soukromých detektivů jednajících jeho jménem, by mohla vycházet z tohoto ustanovení. Pokud však členský stát takovouto výjimku nestanovil, subjekt údajů musí být informován.

Příklad: Ve věci *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*[531] SDEU objasnil, zda právo EU brání předání osobních údajů vnitrostátním orgánem veřejné správy za účelem jejich zpracování jiným orgánem veřejné správy, aniž by byly subjekty údajů informovány o tomto předání a zpracování. V tomto případě vnitrostátní správní agentura předem neinformovala navrhovatele, že předala jejich údaje vnitrostátnímu fondu sociálního zabezpečení.

530 Rozsudek SDEU ze dne 7. listopadu 2013, C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert a další*.

531 Rozsudek SDEU ze dne 1. října 2015, C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*.

SDEU se domníval, že požadavek podle práva EU na informování subjektů údajů o zpracování jejich osobních údajů je „o to důležitější, protože ovlivňuje výkon práva subjektů údajů na přístup ke zpracovávaným údajům a právo na jejich opravu […] a jejich právo vznést námitku proti zpracování těchto údajů". Zásada korektního zpracování vyžaduje, aby byly subjekty údajů informovány o předávání jejich údajů jinému veřejnému subjektu za účelem zpracování tímto jiným subjektem. Podle čl. 13 odst. 1 směrnice 95/46/ES mohou členské státy omezit právo být informován, pokud se to považuje za nezbytné za účelem zajištění důležitého hospodářského zájmu státu, včetně věcí týkajících se zdanění. Tato omezení však musí být uložena legislativními opatřeními. Jelikož žádné legislativní opatření nestanovilo definici údajů, které mají být předány, ani podrobná ujednání pro předání, ale tyto byly stanoveny pouze v protokolu mezi těmito dvěma veřejnými orgány, nebyly splněny podmínky pro odchylku podle práva EU. Navrhovatelé měli být předem informováni o předání svých údajů vnitrostátnímu fondu sociálního zabezpečení a o následném zpracování těchto údajů.

Obsah informací

Podle čl. 8 odst. 1 Modernizované úmluvy č. 108 je správce povinen poskytnout subjektům údajů veškeré informace, které zaručí korektní a transparentní zpracování osobních údajů, včetně:

- totožnosti správce a obvyklého místa pobytu nebo usazení,
- právního základu a účelů zamýšleného zpracování,
- kategorií zpracovávaných osobních údajů,
- případného příjemce nebo kategorií příjemců osobních údajů,
- způsobů, jimiž mohou subjekty údajů vykonávat svá práva.

Podle GDPR platí, že pokud se osobní údaje získávají od subjektu údajů, je správce povinen poskytnout v okamžiku získání osobních údajů subjektu údajů tyto informace:[532]

532 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 1.

- totožnost a kontaktní údaje správce, včetně kontaktních údajů případného pověřence pro ochranu osobních údajů,
- účely zpracování a právní základ pro zpracování, například smlouva nebo právní povinnost,
- oprávněný zájem správce údajů, v případě, že je tento zájem základem pro zpracování,
- koneční příjemci nebo kategorie příjemců osobních údajů,
- to, zda budou osobní údaje předány do třetí země nebo mezinárodní organizaci a zda se toto předání zakládá na rozhodnutí o odpovídající ochraně nebo vychází z vhodných záruk,
- doba, po kterou budou osobní údaje uloženy, nebo není-li tuto dobu možné určit, kritéria použitá pro stanovení doby pro ukládání osobních údajů,
- práva subjektů údajů týkající se přístupu, opravy nebo výmazu a právo omezit zpracování nebo vznést námitku proti zpracování,
- zda je poskytování osobních údajů dáno zákonem nebo smlouvou, zda je subjekt údajů povinen poskytovat své osobní údaje a také důsledky v případě neposkytnutí osobních údajů,
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování,
- právo podat stížnost u dozorového úřadu,
- existence práva odvolat souhlas.

V případech automatizovaného rozhodování, včetně profilování, musí subjekty údajů obdržet smysluplné informace týkající se použitého postupu, jeho významu a předpokládaných důsledků takového zpracování.

V případech, kdy nejsou osobní údaje získávány přímo od subjektu údajů, musí správce údajů oznámit jednotlivci zdroj, ze kterého osobní údaje pocházejí. V každém případě musí správce mimo jiné informovat subjekty údajů o existenci

automatizovaného rozhodování, včetně profilování.[533] V neposlední řadě zásady účelového omezení a transparentnosti vyžadují, aby v případě, že správce zamýšlí zpracovávat osobní údaje pro jiný účel, než který byl původně sdělen subjektu údajů, správce poskytl subjektu údajů informace o tomto novém účelu. Správci musí poskytnout informace před jakýmkoliv dalším zpracováním. Jinými slovy, v případech, kdy subjekt údajů poskytl souhlas se zpracováním osobních údajů, musí správce obdržet obnovený souhlas subjektu údajů, jestliže se změní účel zpracování údajů nebo pokud se rozšíří škála účelů.

Doba poskytování informací

GDPR rozlišuje mezi dvěma scénáři a dvěma okamžiky, kdy musí správce údajů poskytnout informace subjektu údajů:

- Pokud jsou osobní údaje získány přímo od subjektu údajů, musí správce informovat subjekt údajů o všech souvisejících informacích a jeho právech podle GDPR v okamžiku, kdy jsou údaje získány.[534] Pokud má správce v úmyslu dále zpracovávat osobní údaje pro jiný účel, poskytne veškeré relevantní informace před zahájením zpracování.

- Pokud osobní údaje nebyly získány od subjektu údajů přímo, je správce povinen poskytnout informace o zpracování subjektu údajů „v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce" nebo předtím, než jsou údaje sděleny třetí straně.[535]

Vysvětlující zpráva k Modernizované úmluvě č. 108 uvádí, že pokud není informování subjektů údajů možné v okamžiku zahájení zpracování, lze je provést v pozdější fázi, například pokud se z jakéhokoliv důvodu správce obrátí na subjekt údajů.[536]

Různé způsoby poskytování informací

Podle práva RE i EU musí být informace, které je správce povinen poskytovat subjektům údajů, stručné, transparentní, srozumitelné a snadno přístupné. Informace

533 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 a čl. 14 odst. 2 písm. f).

534 Tamtéž, návětí čl. 13 odst. 1 a 2, kde obecné nařízení o ochraně osobních údajů odkazuje na informace o povinnosti, která se uplatní v „okamžiku získání osobních údajů".

535 Tamtéž, čl. 13 odst. 3 a čl. 14 odst. 3; viz také odkaz na „v přiměřených intervalech a bez přílišných průtahů" v Modernizované úmluvě č. 108, čl. 8 odst. 1 písm. b).

536 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 70.

musí být poskytnuty písemně nebo jinými prostředky, včetně v elektronické formě, za použití jasných a jednoduchých jazykových prostředků. Při poskytování informací může správce použít standardizované ikony s cílem poskytnout informace snadno viditelným a srozumitelným způsobem.[537] Například ikona představující zámek může být použita k označení, že údaje jsou shromažďovány bezpečně a/nebo že jsou šifrovány. Subjekty údajů mohou požádat o to, aby jim informace byly sděleny ústně. Informace musí být bezplatné, ledaže jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené (tj. opakují se).[538] Snadný přístup k poskytnutým informacím je stěžejní pro schopnost subjektu údajů vykonávat svá práva svěřená podle práva EU v oblasti ochrany údajů.

Zásada spravedlivého zpracování stanoví, že informace musejí být subjektům údajů snadno srozumitelné. Musí být použity jazykové prostředky, které jsou vhodné pro dané adresáty. Úroveň a druh použitých jazykových prostředků musí být odlišná v závislosti na tom, zda je zamýšleným adresátem například dospělý nebo dítě, široká veřejnost nebo akademický odborník. Otázkou, jak vyvážit tento aspekt srozumitelnosti informací, se zabývá stanovisko pracovní skupiny zřízené podle článku 29 k harmonizovanějším ustanovením pro poskytování informací. Toto stanovisko prosazuje myšlenku takzvaných víceúrovňových sdělení,[539] která umožňují subjektu údajů rozhodnout se, jaké úrovni podrobností dává přednost. Tento způsob poskytování informací však nezbavuje správce povinnosti podle článku 13 a článku 14 GDPR. Správce musí stále subjektu údajů poskytovat veškeré informace.

Jedním z nejúčinnějších způsobů poskytování informací je umístit vhodné informační texty na domovskou stránku správce, například ve formě pravidel ochrany soukromí na webových stránkách. Významná část populace však nepoužívá internet a pravidla společností nebo orgánů veřejné moci týkající se informování by tuto skutečnost měla zohlednit.

537 Evropská komise bude dále rozpracovávat, jaké informace je možné předložit formou ikon, a postupy pro poskytování standardizovaných ikon, a to formou aktů v přenesené pravomoci; viz obecné nařízení o ochraně osobních údajů, čl. 12 odst. 8.

538 Obecné nařízení o ochraně osobních údajů, čl. 12 odst. 1, 5 a 7 a Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. b).

539 Pracovní skupina zřízená podle článku 29 (2004), *Stanovisko 10/2004 k harmonizovanějším ustanovením pro poskytování informací*, WP 100, Brusel, 25. listopadu 2004.

Oznámení o ochraně soukromí při zpracování osobních údajů by na webové stránce mohlo vypadat takto:

Kdo jsme?

„Správcem" zpracování údajů je společnost Bed and Breakfast C&U, usazená v [adresa: xxx], tel.: xxx, fax: xxx, e-mail: info@c&u.com, kontaktní údaje pověřence pro ochranu osobních údajů: [xxx].

Informační oznámení o zpracování osobních údajů je součástí podmínek, jimiž se řídí naše hotelové služby.

Jaké údaje od vás shromažďujeme?

Shromažďujeme od vás tyto osobní údaje: vaše jméno, poštovní adresu, telefonní číslo, e-mailovou adresu, informace o pobytu, číslo kreditní a debetní karty a IP adresy nebo názvy domén počítačů, které jste použili k připojení se na naše webové stránky.

Proč shromažďujeme vaše údaje?

Zpracováváme vaše údaje na základě vašeho souhlasu a pro tyto účely: provedení rezervace, uzavření a plnění smluv souvisejících se službami, které vám nabízíme, a k uspokojení požadavků stanovených právními předpisy, například zákona o místních poplatcích, který nám ukládá povinnost shromažďovat osobní údaje, které umožňují provádět platbu městského poplatku za ubytování.

Jak zpracováváme vaše údaje?

Vaše osobní údaje se uchovávají po dobu tří měsíců. Vaše údaje nejsou předmětem postupů automatizovaného rozhodování.

Naše společnost Bed and Breakfast C&U se důsledně řídí bezpečnostními postupy, které zajišťují, aby vaše osobní informace nebyly poškozeny, zničeny ani zpřístupněny třetí straně bez vašeho svolení a aby se zabránilo neoprávněnému přístupu. Počítače uchovávající informace se nacházejí v zabezpečeném prostředí s omezeným fyzickým přístupem. Používáme zabezpečený

software typu firewall a jiná opatření k omezení elektronického přístupu. Pokud údaje musejí být předány třetí straně, vyžadujeme, aby tato třetí strana měla zavedená podobná opatření na ochranu vašich osobních údajů.

Pohyb veškerých informací, které shromažďujeme nebo uchováváme, je omezen na naše kanceláře. Přístup k osobní údajům je poskytnut pouze osobám, které tyto informace potřebují, aby splnily své povinnosti podle této smlouvy. Výslovně vás požádáme, až budeme potřebovat informace k vaší identifikaci. Je možné, že s námi budete muset spolupracovat při bezpečnostní kontrole, než vám informace zpřístupníme. Osobní informace, které nám poskytnete, můžete kdykoliv aktualizovat tím, že se s námi přímo spojíte.

Jaká jsou vaše práva?

Máte právo na přístup ke svým údajům, na získání kopie svých údajů, na žádost o jejich výmaz nebo opravu nebo na žádost o to, aby vaše údaje byly předány jinému správci.

S žádostmi se na nás můžete obrátit na adrese info@c&u.com. Jsme povinni odpovědět na vaši žádost do jednoho měsíce, ale pokud bude žádost příliš složitá nebo pokud obdržíme příliš mnoho dalších žádostí, budeme vás informovat, že tato lhůta může být prodloužena o další dva měsíce.

Přístup k vašim osobním údajům

Máte právo na přístup ke svým osobním údajům, který se poskytuje na požádání spolu s informacemi o odůvodnění, na němž je zpracování údajů založeno, na žádost o jejich výmaz nebo opravu a právo nebýt předmětem čistě automatizovaného rozhodování, aniž by byly zohledněny vaše názory. S žádostmi se na nás můžete obrátit na adrese info@c&u.com. Máte také právo vznést námitku proti zpracování, odvolat svůj souhlas a podat stížnost u vnitrostátního dozorového úřadu, pokud se domníváte, že toto zpracování údajů je v rozporu s právními předpisy, a pokud chcete požadovat odškodnění za újmu, kterou jste utrpěli v důsledku nezákonného zpracování.

Právo podat stížnost

GDPR ukládá správci povinnost informovat subjekty údajů o vymáhacích mechanismech podle vnitrostátního práva a práva EU v případech porušení zabezpečení osobních údajů. Správce musí informovat subjekty údajů o jejich právu podat stížnost týkající se porušení zabezpečení osobních údajů u dozorového úřadu a v případě nutnosti u vnitrostátního soudu.[540] Právo RE rovněž stanoví právo subjektů údajů být informován o způsobech výkonu svých práv, včetně práva na právní ochranu stanoveného v čl. 9 odst. 1 písm. f).

Výjimky z povinnosti informovat

GDPR stanoví výjimku z povinnosti informovat. Podle čl. 13 odst. 4 a čl. 14 odst. 5 GDPR se povinnost informovat subjekty údajů neuplatní, pokud subjekt údajů již má veškeré relevantní informace.[541] Kromě toho se povinnost informovat neuplatní, pokud byly osobní údaje získány od subjektu údajů a současně není možné informace poskytnout nebo to vyžaduje nepřiměřené úsilí, zejména pak jestliže se osobní údaje zpracovávají pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[542]

Kromě toho mají členské státy podle GDPR prostor pro vlastní uvážení, aby omezily povinnosti a práva svěřená jednotlivcům podle tohoto nařízení, jestliže takové omezení je nezbytné a přiměřené v demokratické společnosti, například s cílem zajistit národní a veřejnou bezpečnost, obranu, ochranu soudních vyšetřování a řízení nebo ochranu hospodářských a finančních zájmů, ale i soukromých zájmů, které jsou závažnější než zájmy v oblasti ochrany údajů.[543]

Veškeré výjimky nebo omezení musí být nezbytné v demokratické společnosti a přiměřené sledovanému cíli. Ve velmi výjimečných případech, například z lékařských důvodů, může samotná ochrana subjektu údajů vyžadovat omezení transparentnosti; to se týká zejména omezení práva na přístup každého subjektu údajů.[544] Jako minimální úroveň ochrany však musí vnitrostátní právo respektovat podstatu

540 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. d) a čl. 14 odst. 2 písm. e); Modernizovaná úmluva č. 108, čl. 8 odst. 1 písm. f).

541 Tamtéž, čl. 13 odst. 4 a čl. 14 odst. 5 písm. a).

542 Tamtéž, čl. 14 odst. 5 písm. b)–e).

543 Obecné nařízení o ochraně osobních údajů, čl. 23 odst. 1.

544 Obecné nařízení o ochraně osobních údajů, článek 15.

základních práv a svobod, které jsou chráněny podle práva EU.[545] K tomu je nutné, aby vnitrostátní právní řád obsahoval konkrétní ustanovení objasňující účel zpracování, kategorie začleněných osobních údajů, záruky a jiné procesní požadavky.[546]

Jsou-li údaje shromažďovány pro účely vědeckého či historického výzkumu, pro statistické účely nebo pro účely archivace, může právo Unie nebo členských států stanovit odchylky od povinnosti informovat, pokud je pravděpodobné, že by tato povinnost znemožnila nebo vážně ohrozila splnění zvláštních účelů.[547]

Podobná omezení existují podle práva RE, kde práva přiznaná subjektům údajů podle článku 9 Modernizované úmluvy č. 108 mohou být za přísných podmínek předmětem případných omezení podle článku 11 Modernizované úmluvy č. 108. Kromě toho podle čl. 8 odst. 2 Modernizované úmluvy č. 108 se povinnost transparentnosti zpracování uložená správcům nepoužije, pokud subjekt údajů již danou informaci má k dispozici.

Právo na přístup k vlastním údajům jednotlivce

V rámci práva RE je právo na přístup k vlastním údajům jednotlivce výslovně uznáno v článku 9 Modernizované úmluvy č. 108. Ten stanoví, že každá osoba má právo získat na požádání informace o zpracování osobních údajů, které se k dané osobě vztahují, a že tyto informace musí být sděleny ve srozumitelné podobě. Právo na přístup bylo uznáno nejen v ustanoveních Modernizované úmluvy č. 108, ale také v judikatuře ESLP. ESLP opakovaně potvrdil, že jednotlivci mají právo na přístup k informacím o svých osobních údajích a že toto právo vyplývá z nutnosti respektovat soukromý život.[548] Právo na přístup k osobním údajům uloženým veřejnými nebo soukromými organizacemi může být za určitých okolností omezeno.[549]

V právu EU je právo na přístup k vlastním údajů výslovně uznáno v článku 15 GDPR a je rovněž vymezeno jako jeden z prvků základního práva na ochranu osobních

545 Obecné nařízení o ochraně osobních údajů, čl. 23 odst. 1.

546 Tamtéž, čl. 23 odst. 2.

547 Tamtéž, čl. 89 odst. 2 a 3.

548 Rozsudek ESLP ze dne 7. července 1989, *Gaskin v. Spojené království*, č. 10454/83; rozsudek ESLP (velkého senátu) ze dne 13. února 2003, *Odièvre v. Francie*, č. 42326/98; rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další v. Slovensko*, č. 32881/04; rozsudek ESLP ze dne 25. září 2012, *Godelli v. Itálie*, č. 33783/09.

549 Rozsudek ESLP ze dne 26. března 1987, *Leander v. Švédsko*, č. 9248/81.

údajů v čl. 8 odst. 2 Listiny základních práv EU.[550] Právo jednotlivce na získání přístupu k vlastním osobním údajům je klíčovým prvkem evropského práva v oblasti ochrany údajů.[551]

GDPR stanoví, že každý subjekt údajů má právo získat přístup ke svým osobním údajům, které musí správci poskytnout.[552] Každý subjekt údajů má zejména právo získat (od správce) potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a informace alespoň o těchto aspektech:

- účely zpracování,
- kategorie dotčených údajů,
- příjemci nebo kategorie příjemců, kterým jsou údaje zpřístupněny,
- doba, po kterou mají být osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby,
- existence práva na opravu nebo výmaz osobních údajů nebo omezení jejich zpracování,
- právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji údajů, které se zpracovávají, pokud nejsou získány od subjektu údajů,
- v případě automatizovaných rozhodnutí smysluplné informace týkající se automatizovaného zpracování údajů.

Správce údajů musí subjektu údajů poskytnout kopii zpracovávaných osobních údajů. Veškeré informace sdělené subjektu údajů musí být poskytnuty srozumitelnou formou, což znamená, že správce musí zajistit, že subjekt údajů dokáže

550 Viz také rozsudek SDEU ze dne 17. července 2014, spojené věci C-141/12 a C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* a *Minister voor Immigratie, Integratie en Asiel v. M a S*; rozsudek SDEU ze dne 16. července 2015, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. Evropský úřad pro bezpečnost potravin (EFSA), Evropská komise*.

551 Rozsudek SDEU ze dne 17. července 2014, spojené věci C-141/12 a C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* a *Minister voor Immigratie, Integratie en Asiel v. M a S*.

552 Obecné nařízení o ochraně osobních údajů, čl. 15 odst. 1.

porozumět poskytnutým informacím. Například použití odborných zkratek, nesrozumitelných pojmů nebo zkratek v odpovědi na žádost o přístup obvykle nebude vyhovovat, ledaže je vysvětlen význam těchto pojmů. Pokud se provádí automatizované rozhodování, včetně profilování, bude nutné vysvětlit obecné principy, jimiž se automatizované rozhodování řídí, včetně kritérií, která byla zvažována při hodnocení subjektu údajů. Podobná ustanovení existují i podle **práva RE**.[553]

Příklad: Přístup k vlastním osobním údajům pomůže subjektu údajů zjistit, zda jsou údaje přesné, či nikoliv. Je proto zásadní, aby byl subjekt údajů srozumitelnou formou informován, nejen o vlastních osobních údajích, které se zpracovávají, ale také o kategoriích, v jejichž rámci se tyto osobní údaje zpracovávají, jako je jméno, IP adresa, geolokalizační souřadnice, číslo kreditní karty atd.

V odpovědi na žádost o přístup musí být uvedeny informace o zdroji údajů – pokud údaje nejsou získávány od subjektu údajů – pokud jsou tyto informace dostupné. Toto ustanovení je třeba chápat v kontextu zásad korektnosti, transparentnosti a odpovědnosti. Správce nesmí zničit informace o zdroji údajů, aby byl vyňat z povinnosti je sdělovat – ledaže by tento výmaz proběhl navzdory obdržení žádosti o přístup – a musí být stále v souladu s obecnými požadavky na „odpovědnost".

Jak je stanoveno v judikatuře SDEU, právo na přístup k osobním údajům nesmí být neoprávněně omezeno časovými omezeními. Subjekty údajů musí mít přiměřenou možnost získat informace o operacích zpracování údajů, které proběhly v minulosti.

Příklad: Ve věci *Rijkeboer*[554] byl SDEU požádán, aby určil, zda právo jednotlivce na přístup k informacím o příjemcích nebo kategoriích příjemců osobních údajů a obsahu údajů může být omezeno na období jednoho roku předcházejícího žádosti jednotlivce o přístup.

K určení, zda právní předpisy EU opravňují ke stanovení takovéhoto časového omezení, se SDEU rozhodl, že vyloží článek 12 s ohledem na účely směrnice. SDEU nejprve uvedl, že právo na přístup je nutné k tomu, aby byl subjektu údajů umožněn výkon práv v tom smyslu, aby mohli přimět správce opravit,

553 Modernizovaná úmluva č. 108, čl. 8 odst. 1 písm. c).

554 Rozsudek SDEU ze dne 7. května 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*.

vymazat nebo zablokovat údaje nebo oznámit třetím stranám, jimž byly údaje zpřístupněny, veškeré opravy, výmazy nebo blokování. Účinné právo na přístup je také nezbytné k tomu, aby subjekt údajů mohl vykonávat své právo podat námitku proti zpracovávání svých osobních údajů nebo právo podat stížnost nebo požadovat náhradu škody.[555]

Aby byl zajištěn praktický účinek práv přiznaných subjektům údajů, rozhodl SDEU, že „se toto právo minulosti nutně týkat musí. Pokud by totiž tomu tak nebylo, dotčená osoba by nebyla s to účinně uplatňovat své právo na opravu, výmaz nebo blokování údajů, jež považuje za nepřípustné nebo nesprávné, jakož i právo na soudní ochranu pro případ utrpěné škody."

6.1.2. Právo na opravu

Podle práva EU a **práva RE** mají subjekty údajů právo na opravu svých osobních údajů. Přesnost osobních údajů je zásadní pro účely zajištění vysoké úrovně ochrany údajů subjektů údajů.[556]

Příklad: Ve věci *Ciubotaru v. Moldavsko*[557] stěžovatel nebyl schopen změnit registraci své národnosti v úředních záznamech z moldavské na rumunskou, a to údajně kvůli skutečnosti, že svou žádost nedoložil. ESLP považoval za přijatelné, aby státy při registraci národnosti jednotlivce požadovaly objektivní důkazy. Pokud by bylo toto tvrzení založeno pouze na subjektivních a nepodložených důvodech, mohly by je orgány zamítnout. Tvrzení žadatele však bylo založeno na více než subjektivním vnímání vlastní národnosti; byl schopen doložit objektivně ověřitelné vazby na rumunskou národnost, jako je jazyk, jméno, empatie a jiné. Přesto podle vnitrostátního práva musel stěžovatel poskytnout důkazy, že jeho rodiče náleželi k rumunské národnosti. Vzhledem k historickým skutečnostem v Moldavsku vytvořil tento požadavek nepřekonatelnou překážku pro registraci jiné národnosti, než jakou zaznamenaly sovětské orgány v případě jeho rodičů. Stát tím, že zabránil stěžovateli dosáhnout přezkumu svého tvrzení s ohledem na

555 Obecné nařízení o ochraně osobních údajů, čl. 15 odst. 1 písm. c) a f), článek 16, čl. 17 odst. 2 a článek 21 a kapitola VIII.

556 Tamtéž, článek 16 a 65. bod odůvodnění; Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. e).

557 Rozsudek ESLP ze dne 27. dubna 2010, *Ciubotaru v. Moldavsko*, č. 27138/04, body 51 a 59.

objektivně ověřitelné důkazy, nesplnil svou pozitivní povinnost zabezpečit, aby byl účinně respektován soukromý život stěžovatele. Soud rozhodl, že došlo k porušení článku 8 EÚLP.

V některých případech bude postačovat, aby subjekt údajů jednoduše požádal o opravu, například způsob zápisu jména, změna adresy nebo telefonního čísla. Podle **práva EU** i **práva RE** musí být nepřesné osobní údaje opraveny bez zbytečného odkladu nebo přílišných průtahů.[558] Pokud jsou však takovéto žádosti spojeny s právně závažnými skutečnostmi, jako je právní identita subjektu údajů, nebo správní místo pobytu pro zasílání právních dokumentů, nemusí žádosti o opravu postačovat a správce může být oprávněn požadovat důkaz o údajné nepřesnosti. Tyto požadavky nesmí představovat pro subjekt údajů nepřiměřené důkazní břemeno, a tím bránit subjektům údajů v tom, aby dosáhly opravy svých údajů. ESLP dospěl k závěru, že došlo k porušení článku 8 EÚLP v několika věcech, kdy stěžovatel nebyl schopen napadnout přesnost informací uchovávaných v tajných registrech.[559]

Příklad: Ve věci *Cemalettin Canli v. Turecko*[560] dospěl ESLP k závěru, že došlo k porušení článku 8 EÚLP kvůli nesprávnému informování v trestním řízení ze strany policie.

Stěžovatel byl dvakrát předmětem trestního řízení kvůli údajnému členství v ilegálních organizacích, ale nebyl odsouzen. Poté, co byl stěžovatel znovu zadržen a obviněn z jiného trestného činu, předložila policie trestnímu soudu zprávu s názvem „*informační formulář o dalších trestných činech*", v němž se uvádělo, že stěžovatel byl členem dvou nelegálních organizací. Žádost stěžovatele, aby byla zpráva a policejní záznamy změněny, byla zamítnuta. ESLP rozhodl, že informace v dané policejní zprávě spadají do působnosti článku 8 EÚLP, protože systematicky shromažďované veřejné informace uložené ve spisech v držení orgánů by mohly spadat do působnosti pojmu „soukromý život". Kromě toho byla policejní zpráva nesprávně sepsána a její předložení trestnímu soudu nebylo v souladu s vnitrostátním právem. Soud rozhodl, že došlo k porušení článku 8.

558 Obecné nařízení o ochraně osobních údajů, článek 16; Modernizovaná úmluva č. 108, čl. 9 odst. 1.

559 Rozsudek ESLP (velkého senátu) ze dne 4. května 2000, *Rotaru v. Rumunsko*, č. 28341/95.

560 Rozsudek ESLP ze dne 18. listopadu 2008, *Cemalettin Canli v. Turecko*, č. 22427/04, body 33 a 42–43; rozsudek ESLP ze dne 2. února 2010, *Dalea v. Francie*, č. 964/07.

Během občanskoprávního sporu nebo řízení u orgánu veřejné moci za účelem rozhodnutí, zda jsou údaje správné, či nikoliv, může subjekt údajů požádat o vložení záznamu nebo poznámky do svého spisu, v níž se uvádí, že se popírá přesnost údajů a že se vyčkává na přijetí úředního rozhodnutí.[561] Během tohoto období nesmí správce údajů předkládat údaje jakožto správné údaje nepodléhající změně, a zejména ne třetím stranám.

6.1.3. Právo na výmaz („právo být zapomenut“)

To, že subjekty údajů získaly právo dosáhnout výmazu vlastních údajů, je zvlášť důležité pro účinné uplatňování zásad ochrany údajů, zejména pak zásady minimalizace údajů (osobní údaje musí být omezeny na to, co je nezbytné pro účely, pro které se tyto údaje zpracovávají). Právo na výmaz se proto nachází v právních nástrojích RE i EU.[562]

Příklad: Ve věci *Segerstedt-Wiberg a další v. Švédsko*[563] byli stěžovatelé členy některých liberálních a komunistických politických stran. Měli podezření, že informace o nich byly zapsány do bezpečnostních policejních záznamů, a požádali o jejich výmaz. ESLP byl uspokojen, že ukládání dotčených údajů má právní základ a sleduje legitimní cíl. Avšak u některých těchto stěžovatelů ESLP shledal, že další uchovávání údajů není přiměřeným zásahem do jejich soukromého života. Například v případě jednoho stěžovatele uchovávaly orgány informaci o tom, že v roce 1969 údajně hájil násilný odpor vůči policejnímu dohledu na demonstracích. ESLP shledal, že tato informace nemůže představovat relevantní zájem národní bezpečnosti, zejména vzhledem k její historické povaze. Soud konstatoval, že došlo k porušení článku 8 EÚLP, pokud jde o čtyři z pěti stěžovatelů, protože vzhledem k tomu, že se údajné činy stěžovatelů odehrály před velmi dlouhou dobou, není další ukládání jejích údajů relevantní.

Příklad: Ve věci *Brunet v. Francie*[564] stěžovatel zažaloval uchovávání jeho osobních údajů v policejní databázi, která obsahovala informace o odsouzených, obviněných a obětech. Ačkoliv bylo trestní řízení proti stěžovateli zastaveno, v databázi se nacházely jeho údaje. ESLP shledal, že došlo k porušení

561 Obecné nařízení o ochraně osobních údajů, článek 18 a 67. bod odůvodnění.

562 Tamtéž, článek 17.

563 Rozsudek ESLP ze dne 6. června 2006, *Segerstedt-Wiberg a další v. Švédsko*, č. 62332/00, body 89 a 90; viz také například rozsudek ESLP ze dne 18. dubna 2013, *M.K. v. Francie*, č. 19522/09.

564 Rozsudek ESLP ze dne 18. září 2014, *Brunet v. Francie*, č. 21010/10.

článku 8 EÚLP. Předtím, než soud dospěl k tomuto závěru, vzal v potaz, že v praxi neměl stěžovatel možnost dosáhnout výmazu svých osobních údajů z databáze. ESLP rovněž vzal v úvahu povahu informací obsažených v databázi a měl za to, že se jednalo o narušení soukromí stěžovatele, protože zde byly obsaženy údaje o jeho totožnosti a osobnosti. Kromě toho konstatoval, že doba uchovávání osobních záznamů v databázi, která činila 20 let, byla nepřiměřeně dlouhá, zejména vzhledem k tomu, že stěžovatele nikdy neodsoudil žádný soud.

Modernizovaná úmluva č. 108 výslovně uznává, že každý jednotlivec má právo docílit výmazu údajů, které jsou nebo byly nepřesné, nepravdivé nebo byly zpracovávány protiprávně.[565]

V právu EU vychází žádosti subjektů údajů o výmaz údajů z článku 17 GDPR. Právo na to, aby byly bez zbytečného odkladu vymazány osobní údaje daného jednotlivce, platí, pokud:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas, na jehož základě probíhalo zpracovávání, a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 GDPR.[566]

565 Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. e).

566 Obecné nařízení o ochraně osobních údajů, čl. 17 odst. 1.

Důkazní břemeno, že je zpracování údajů oprávněné, ponesou správci údajů, protože jsou zodpovědní za zákonnost zpracování.[567] Podle zásady odpovědnosti musí být správce kdykoliv schopen doložit, že jeho zpracování údajů má solidní právní základ, jinak musí být zpracování zastaveno.[568] GDPR vymezuje výjimky z práva být zapomenut, včetně případu, kdy je zpracování osobních údajů nezbytné:

- pro výkon práva na svobodu projevu a informace,
- pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,
- z důvodů veřejného zájmu v oblasti veřejného zdraví,
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely,
- pro určení, výkon nebo obhajobu právních nároků.[569]

SDEU potvrdil význam práva na výmaz pro zajištění vysoké úrovně ochrany údajů.

Příklad: Ve věci *Google Spain*[570] se SDEU zabýval tím, zda byla společnost Google povinna vymazat zastaralé informace týkající se finančních potíží stěžovatele ze seznamu výsledků vyhledávání. Kromě jiného společnost Google napadla, že je odpovědným subjektem, a namítala, že pouze poskytuje odkaz na webovou stránku vydavatele, na které jsou informace umístěny, v tomto případě na novinovou zprávu o problémech stěžovatele v souvislosti

567 Tamtéž.

568 Tamtéž, čl. 5 odst. 2.

569 Tamtéž, čl. 17 odst. 3.

570 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, body 55–58.

s úpadkem.[571] Společnost Google namítala, že žádost o výmaz zastaralých informací z webové stránky by měla být podána osobě, která je umísťuje na webové stránky, a nikoliv společnosti Google, která pouze poskytuje odkaz na původní stránku. SDEU dospěl k závěru, že se společnost Google při prohledávání webu za účelem nalezení informací a webových stránek a při indexaci obsahu za účelem poskytování výsledků vyhledávání stala správcem údajů, na kterého se vztahují odpovědnost a povinnosti podle práva EU.

SDEU objasnil, že internetové vyhledávače a výsledky vyhledávání poskytující osobní údaje mohou sestavit podrobný profil jednotlivce.[572] Vyhledávače činí informace obsažené v takovém seznamu výsledků všudypřítomnými. S ohledem na možnou závažnost takového zásahu tento zásah nelze odůvodnit pouze hospodářským zájmem provozovatele vyhledávače na takovém zpracování. Je třeba hledat spravedlivou rovnováhu zejména mezi legitimním zájmem uživatelů internetu na přístupu k této informaci a základními právy subjektu údajů plynoucími z článků 7 a 8 Listiny základních práv EU. Ve stále digitalizovanější společnosti je požadavek na to, aby byly osobní údaje přesné a nepřekračovaly míru toho, co je nezbytné (například pro informování veřejnosti), zásadní pro zajištění vysoké úrovně ochrany údajů jednotlivců. „[S]právce odpovědný za dané zpracování, [musí] v rámci své odpovědnosti, pravomoci a možností zajistit, aby toto zpracování splňovalo požadavky“ práva EU tak, aby zavedené právní záruky měly plný účinek.[573] To znamená, že právo dosáhnout výmazu vlastních osobních údajů, pokud je zpracování zastaralé nebo již není nezbytné, rovněž zahrnuje správce údajů, kteří danou informaci replikují.[574]

571 Společnost Google rovněž napadla to, že se na ni použijí pravidla EU v oblasti ochrany údajů, a to vzhledem ke skutečnosti, že společnost Google Inc. je usazena ve Spojených státech a zpracování v této věci dotčených osobních údajů bylo rovněž prováděno ve Spojených státech. Druhý argument pro to, že se neuplatní právo EU v oblasti ochrany údajů, souvisel s tvrzením, že vyhledávače nelze považovat za „správce“ s ohledem na údaje zobrazené ve výsledcích vyhledávání, neboť o uvedených údajích nevědí a nemají nad nimi kontrolu. Oba argumenty SDEU zamítl a rozhodl, že směrnice 95/46/ES byla v takovém případě použitelná, a dále zkoumal oblast působnosti práv, která tato směrnice zaručovala, zejména práva na výmaz osobních údajů.

572 Tamtéž, body 36, 38, 80–81 a 97.

573 Tamtéž, body 81–83.

574 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, bod 88. Viz také pracovní skupina zřízená podle článku 29 (2014), *Guidelines on the implementation of the CJEU judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12 [Pokyny k provádění rozsudku SDEU ve věci „Google Spain a Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González“ C-131/12]*, WP 225, Brusel, 26. listopadu 2014 a doporučení Výboru ministrů členským státům CM/Rec2012(3) o ochraně lidských práv ve vztahu k internetovým vyhledávačům, 4. dubna 2012.

Při úvahách, zda je či není společnost Google povinna odstranit odkazy související se stěžovatelem, SDEU konstatoval, že za určitých podmínek mají jednotlivci právo podat žádost o výmaz osobních údajů. Toto právo může být uplatněno, pokud informace týkající se daného jednotlivce jsou nepřesné, nepřiměřené, nepodstatné a přesahují míru s ohledem na účely zpracování údajů. SDEU uznal, že toto právo není absolutní. Musí být vyváženo jinými právy a zájmy, zejména zájmem veřejnosti mít přístup k určitým informacím. Každá žádost o výmaz musí být posouzena jednotlivě, aby bylo dosaženo rovnováhy mezi základními právy na ochranu osobních údajů a soukromým životem subjektu údajů na straně jedné a oprávněnými zájmy všech uživatelů internetu, včetně vydavatelů, na straně druhé. SDEU poskytl pokyny k faktorům, které je třeba zvážit při provádění tohoto poměřování. Zvlášť důležitým prvkem je povaha dotčené informace. Pokud se informace týkají soukromého života jednotlivce a neexistuje veřejný zájem na dostupnosti této informace, převažuje ochrana údajů a soukromí nad právem široké veřejnosti mít přístup k daným informacím. Naopak pokud se jeví, že subjekt údajů je veřejně známá osobnost nebo že informace je takové povahy, že je odůvodněna její dostupnost široké veřejnosti, pak je zásah do základních práv subjektu údajů na ochranu údajů a soukromí odůvodněný převažujícím zájmem široké veřejnosti mít k dotčené informaci přístup.

V návaznosti na vynesení tohoto rozsudku přijala pracovní skupina zřízená podle článku 29 pokyny k provádění tohoto rozsudku SDEU.[575] Součástí pokynů je seznam společných kritérií, která mají dozorové úřady použít při vyřizování stížností souvisejících s žádostmi jednotlivců o výmaz, a je zde vysvětleno, co toto právo na výmaz obnáší, a jsou uvedeny pokyny k tomuto poměřování práv. V pokynech se opakuje, že tato posouzení musí být prováděna zvlášť pro každý jednotlivý případ. Jelikož právo být zapomenut není absolutní, může se výsledek žádosti lišit v závislosti na daném případě. To lze doložit judikaturou SDEU po rozsudku ve věci Google.

575 Pracovní skupina zřízená podle článku 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 [Pokyny k provádění rozsudku SDEU ve věci „Google Spain a Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12]*, WP 225, Brusel, 26. listopadu 2014.

Příklad: Ve věci *Camera di Commercio di Lecce v. Manni*[576] SDEU musel přezkoumat, zda má jednotlivec právo dosáhnout výmazu svých osobních údajů zveřejněných ve veřejném rejstříku společností, jakmile jeho společnost přestala existovat. Pan Manni požádal obchodní komoru v Lecce, aby vymazala jeho osobní údaje z tohoto rejstříku poté, co zjistil, že případní klienti mohou nahlížet do rejstříku a dozvědět se, že byl dříve jednatelem společnosti, která před více než deseti lety vyhlásila úpadek. Stěžovatel byl přesvědčen, že by tato informace případné klienty odradila.

Při poměřování práva pana Manniho na ochranu jeho osobních údajů se zájmem široké veřejnosti na přístupu k informacím SDEU nejprve přezkoumal účel veřejného rejstříku. Poukázal na skutečnost, že zveřejnění je stanoveno zákonem, a zejména směrnicí EU, která má za cíl učinit informace o společnostech snáze přístupnými třetím stranám. Třetí strany by tudíž měly mít přístup a být schopny přezkoumat základní listiny společnosti a jiné informace o ní, „zejména [...] údaj[e] o osobách, které jsou oprávněny společnost zavazovat". Účelem zveřejnění bylo také zaručit právní jistotu s ohledem na intenzivnější obchod mezi členskými státy, a to zajištěním, že třetí strany budou mít přístup ke všem relevantním informacím o společnostech v celé EU.

SDEU dále konstatoval, že i po uplynutí určité doby a i po likvidaci společnosti často stále přetrvávají práva a právní povinnosti související s danou společností. Spory související s likvidací mohou být vleklé a i řadu let po ukončení existence společnosti mohou vyvstat otázky týkající se určité společnosti, jejích vedoucích pracovníků a likvidátorů. SDEU konstatoval, že vzhledem k četnosti možných scénářů a k rozdílným promlčecím lhůtám stanoveným jednotlivými členskými státy „se za současného stavu jeví nemožné určit jedinou lhůtu od okamžiku likvidace společnosti, po jejímž uplynutí by zápis uvedených údajů v rejstříku a jejich zveřejňování nebyly dále nutné". Vzhledem k legitimnímu cíli, jímž je zveřejnění, a k potížím při stanovování lhůty, po jejímž uplynutí by bylo možné osobní údaje vymazat z rejstříku, aniž by byly poškozeny zájmy třetích stran, SDEU konstatoval, že pravidla EU v oblasti ochrany údajů nezaručují právo na výmaz osobních údajů u osob v situaci pana Manniho.

576 Rozsudek SDEU ze dne 9. března 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*.

Pokud správce zveřejnil osobní údaje a je povinen tyto informace vymazat, je správce údajů povinen a musí přijmout „vhodné“ kroky s cílem informovat správce, kteří tyto údaje zpracovávají, o žádosti subjektu údajů o výmaz. Činnosti správce musí zohlednit dostupné technologie a náklady na provedení.[577]

6.1.4. Právo na omezení zpracování

Článek 18 GDPR přiznává subjektům údajů pravomoc dočasně zabránit správci zpracovávat jejich osobní údaje. Subjekty údajů mohou požádat správce, aby omezil zpracování, pokud:

- je popírána přesnost osobních údajů,
- zpracování je protiprávní a subjekt údajů namísto o výmaz osobních údajů žádá o omezení jejich použití,
- údaje musí být uchovávány pro výkon nebo obhajobu právních nároků,
- dosud nebylo přijato rozhodnutí o tom, zda oprávněné důvody správce údajů převažují nad důvody subjektu údajů.[578]

Způsoby, jak může správce omezit zpracování osobních údajů, mohou například zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění údajů uživatelům nebo dočasné odstranění osobních údajů.[579] Správce musí upozornit subjekt údajů předem na to, že bude omezení zpracování zrušeno.[580]

Oznamovací povinnost v souvislosti s opravou nebo výmazem osobních údajů nebo omezení zpracování

Správce musí oznámit jednotlivým příjemcům, jimž zpřístupnil osobní údaje, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování s výjimkou případů, není-li to nemožné nebo nevyžaduje-li to nepřiměřené úsilí.[581] Pokud sub-

577 Obecné nařízení o ochraně osobních údajů, čl. 17 odst. 2 a 66. bod odůvodnění.

578 Tamtéž, čl. 18 odst. 1.

579 Tamtéž, 67. bod odůvodnění.

580 Tamtéž, čl. 18 odst. 3.

581 Tamtéž, článek 19.

jekt údajů požaduje informace o těchto příjemcích, musí mu správce tuto informaci poskytnout.[582]

6.1.5. Právo na přenositelnost údajů

Podle GDPR požívají subjekty údajů práva na přenositelnost údajů v situacích, kdy se osobní údaje, které poskytly správci, zpracovávají automatizovaně na základě souhlasu, nebo pokud je zpracování osobních údajů nezbytné pro plnění smlouvy a je prováděno automatizovaně. To znamená, že právo na přenositelnost údajů se nepoužije v situacích, kdy je zpracování osobních údajů založeno na jiném právním základě, než je souhlas nebo smlouva.[583]

Pokud se použije právo na přenositelnost údajů, mají subjekty údajů právo na to, aby jejich osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.[584] K usnadnění tohoto předávání by správce měl vyvinout interoperabilní formáty umožňující přenositelnost údajů pro subjekty údajů.[585] GDPR stanoví, že tyto formáty musí být strukturované, běžně používané a strojově čitelné s cílem usnadnit interoperabilitu.[586] Interoperabilitu lze vymezit v širokém smyslu jako schopnost informačních systémů provádět výměnu údajů a umožňovat sdílení informací.[587] Zatímco účelem používaných formátů je dosažení interoperability, GDPR nestanoví konkrétní doporučení ohledně konkrétního formátu, který je třeba poskytnout: formáty se mohou v jednotlivých odvětvích lišit.[588]

Podle pokynů pracovní skupiny zřízené podle článku 29 právo na přenositelnost údajů „podporuje uživatelskou volbu a kontrolu a rovněž posílení pravomocí uživatelů“ a jeho cílem je svěřit subjektům údajů kontrolu nad jejich vlastními osobními údaji.[589] Pokyny objasňují hlavní prvky přenositelnosti údajů, k nimž patří:

582 Tamtéž.

583 Tamtéž, 68. bod odůvodnění a čl. 20 odst. 1.

584 Tamtéž, čl. 20 odst. 2.

585 Tamtéž, 68. bod odůvodnění a čl. 20 odst. 1.

586 Tamtéž, 68. bod odůvodnění.

587 Evropská komise, sdělení ze dne 2. dubna 2016 s názvem Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final.

588 Pracovní skupina zřízená podle článku 29 (2016), *Pokyny týkající se práva na přenositelnost údajů*, WP 242, 13. prosince 2016 a revidováno dne 5. dubna 2017, s. 13.

589 Tamtéž.

- právo subjektů údajů získat vlastní osobní údaje zpracovávané správcem ve strukturovaném, běžně používaném a strojově čitelném a interoperabilním formátu,

- právo předat osobní údaje od jednoho správce údajů jinému správci údajů bez překážek, je-li to technicky proveditelné,

- režim kontroly – pokud správce odpovídá na žádost o přenositelnost údajů, jedná z pokynu subjektu údajů, což znamená, že není zodpovědný za to, zda příjemce dodržuje právní předpisy v oblasti ochrany údajů, jelikož o tom, komu se údaje předávají, rozhoduje subjekt údajů,

- výkonem práva na přenositelnost údajů nesmí být dotčeno žádné jiné právo, jak je tomu i u veškerých ostatních práv uvedených v GDPR.

6.1.6. Právo vznést námitku

Subjekty údajů mohou uplatnit své právo vznést námitku proti zpracování osobních údajů z důvodů souvisejících s jejich konkrétní situací a proti zpracovávání údajů pro účely přímého marketingu. Právo vznést námitku lze vykonávat automatizovanými prostředky.

Právo vznést námitku z důvodů souvisejících s konkrétní situací subjektů údajů

Subjekty údajů nemají obecné právo vznést námitku proti zpracování svých údajů.[590] Článek 21 odst. 1 GDPR přiznává subjektu údajů pravomoc vznést námitku z důvodů týkajících se jeho konkrétní situace v případě, že právním základem zpracování je to, že správce plní úkol ve veřejném zájmu, nebo je zpracování založeno na oprávněných zájmech správce.[591] Právo vznést námitku se týká činností profilování. Podobné právo uznává Modernizovaná úmluva č. 108.[592]

590 Viz také rozsudek ESLP ze dne 27. srpna 1997, *M.S. v. Švédsko*, č. 20837/92 (kde byly sděleny lékařské údaje bez souhlasu nebo možnosti vznést námitku); rozsudek ESLP ze dne 26. března 1987, *Leander v. Švédsko*, č. 9248/81; rozsudek ESLP ze dne 10. května 2011, *Mosley v. Spojené království*, č. 48009/08.

591 Obecné nařízení o ochraně osobních údajů, 69. bod odůvodnění a čl. 6 odst. 1 písm. e) a f).

592 Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. d); doporučení o profilování, článek 5.3.

Právo vznést námitku z důvodů týkajících se konkrétní situace subjektu údajů má za cíl dosáhnout vhodné rovnováhy mezi právy subjektu údajů na ochranu údajů a legitimními právy jiných osob při zpracování jejich údajů. SDEU však objasnil, že práva subjektu údajů obecně převažují nad hospodářskými zájmy správce údajů v závislosti na „povaze dotčené informace a její citlivosti v souvislosti se soukromím subjektu údajů, jakož i na zájmu veřejnosti mít k této informaci přístup".[593] Podle GDPR nesou důkazní břemeno správci, kteří musejí prokázat přesvědčivé důvody pro další zpracování.[594] Podobně Vysvětlující zpráva k Modernizované úmluvě č. 108 objasňuje, že oprávněné důvody pro zpracování údajů (které mohou převažovat nad právem subjektů údajů vznést námitku) budou muset být prokázány individuálně.[595]

Příklad: Ve věci *Manni*[596] SDEU rozhodl, že vzhledem k legitimnímu účelu zpřístupnění osobních údajů v rejstříku společností, a zejména vzhledem k nutnosti chránit zájmy třetích stran a zajistit právní jistotu, pan Manni v zásadě neměl právo dosáhnout výmazu svých osobních údajů z rejstříku společností. SDEU však uznal existenci práva podat námitku proti zpracování tím, že konstatoval, že „není možné vyloučit, že mohou existovat zvláštní situace, v nichž vážné a legitimní důvody související s konkrétní situací subjektu údajů výjimečně odůvodňují, aby byl po uplynutí dostatečně dlouhé doby [...] omezen přístup k osobním údajům zapsaným v rejstříku [...] třetím osobám, které prokáží zvláštní zájem na nahlížení do těchto údajů".

SDEU se domníval, že je věcí vnitrostátních soudů, aby jednotlivé případy posoudily a vzaly přitom v úvahu příslušné okolnosti daného jednotlivce a to, zda existovaly legitimní a převažující důvody, které by mohly výjimečně odůvodnit omezený přístup třetích stran k osobním údajům obsaženým v rejstřících společností. Objasnil však, že ve věci pana Manniho nelze považovat pouhou skutečnost, že zpřístupnění jeho osobních údajů v rejstříku údajně ovlivnilo jeho klientelu, za legitimní a vážný důvod. Případní klienti pana Manniho mají oprávněný zájem mít přístup k informacím o úpadku jeho někdejší společnosti.

593 Rozsudek SDEU (velkého senátu) ze dne 13. května 2014, C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, bod 81.

594 Viz také Modernizovanou úmluvu č. 108, čl. 98 odst. 1 písm. d), kde se uvádí, že subjekt údajů může vznést námitku proti zpracování svých údajů, „pokud správce neuvede zákonné důvody pro zpracování, které mají přednost před zájmy nebo právy a základními svobodami dané osoby".

595 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 78.

596 Rozsudek SDEU ze dne 9. března 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, body 47 a 60.

Účinek úspěšné námitky je ten, že správce již nesmí zpracovávat dotčené údaje. Operace zpracování prováděné s údaji daného subjektu údajů před podáním námitky jsou však i nadále legitimní.

Právo vznést námitku ohledně použití údajů pro účely přímého marketingu

Článek 21 odst. 2 GDPR stanoví zvláštní právo podat námitku proti použití osobních údajů pro účely přímého marketingu, čímž se dále vyjasňuje článek 13 směrnice o soukromí a elektronických komunikacích. Toto právo je také stanoveno v Modernizované úmluvě č. 108, jakož i v doporučení RE k přímému marketingu.[597] Vysvětlující zpráva k Modernizované úmluvě č. 108 objasňuje, že námitky proti zpracování údajů pro účely přímého marketingu by měly vést k bezpodmínečnému výmazu nebo odstranění dotčených osobních údajů.[598]

Subjekt údajů má právo kdykoliv a bezplatně vznést námitku proti použití jeho osobních údajů pro účely přímého marketingu. Subjekty údajů musí být o tomto právu informovány zřetelně a odděleně od jakýchkoli jiných informací.

Právo vznést námitku automatizovanými prostředky

Pokud jsou osobní informace používány a zpracovávány pro účely služeb informační společnosti, může subjekt údajů uplatnit své právo podat námitku proti zpracování svých osobních údajů automatizovanými prostředky.

Služby informační společnosti jsou definovány jako každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.[599]

Správci údajů nabízející služby informační společnosti musí mít zavedená technická ustanovení a postupy s cílem zajistit, že právo vznést námitku automatizovanými prostředky může být účinně vykonáváno.[600] Může se například jednat o blokování tzv. cookies na webových stránkách nebo vypnutí sledování v internetovém prohlížeči.

597 Rada Evropy, Výbor ministrů (1985), Doporučení Rec(85)20 členským státům ze dne 25. října 1985 o ochraně osobních údajů používaných pro účely přímého marketingu, čl. 4 odst. 1.

598 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 79.

599 Směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice 98/48/ES, čl. 1 odst. 2.

600 Obecné nařízení o ochraně osobních údajů, čl. 21 odst. 5.

Právo vznést námitku pro účely vědeckého či historického výzkumu nebo pro statistické účely

Podle práva EU by měl být vědecký výzkum vykládán v širokém smyslu a zahrnuje například technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný výzkum a výzkum financovaný ze soukromých zdrojů.[601] Historický výzkum rovněž zahrnuje výzkum pro genealogické účely, přičemž je třeba mít na paměti, že by se toto nařízení nemělo vztahovat na zesnulé osoby.[602] Statistickými účely se rozumí jakékoli operace shromažďování a zpracování osobních údajů nezbytné pro statistická zjišťování nebo pro generování statistických výsledků.[603] I zde platí, že konkrétní situace subjektu údajů je právním základem, pokud jde o právo vznést námitku proti zpracování osobních údajů pro účely výzkumu.[604] Jedinou výjimku tvoří nezbytnost zpracování pro účely plnění úkolu prováděného z důvodů veřejného zájmu. Právo na výmaz však neplatí, pokud je zpracování nezbytné (z důvodů veřejného zájmu či z jiných důvodů) pro účely vědeckého či historického výzkumu či pro statistické účely.[605]

GDPR stanoví rovnováhu mezi požadavky vědeckého, statistického či historického výzkumu a právy subjektů údajů a nabízí konkrétní záruky a odchylky v článku 89. Právo Unie či členského státu tedy může stanovit odchylky od práva vznést námitku, pokud je pravděpodobné, že by dané právo znemožnilo nebo vážně ohrozilo splnění zvláštních účelů, a pokud tyto odchylky jsou pro splnění těchto účelů nezbytné.

V rámci **práva RE** stanoví čl. 9 odst. 2 Modernizované úmluvy č. 108, že omezení práv subjektu údajů, včetně práva vznést námitku, může být stanoveno zákonem týkajícím se zpracování údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, jestliže neexistuje nebezpečí porušení práv a základních svobod subjektů údajů.

Avšak Vysvětlující zpráva (bod 41) rovněž uznává, že by subjekty údajů měly mít příležitost udělit souhlas pouze pro některé oblasti výzkumu nebo pro části výzkumných projektů v rozsahu, v jakém to zamýšlený účel umožňuje, a podat námitku

601 Tamtéž, 159. bod odůvodnění.
602 Tamtéž, 160. bod odůvodnění.
603 Tamtéž, 162. bod odůvodnění.
604 Tamtéž, čl. 21 odst. 6.
605 Tamtéž, čl. 17 odst. 3 písm. d).

v případě, že mají za to, že zpracování nadměrně zasahuje do jejich práv a svobod bez legitimního důvodu.

Jinými slovy by takové zpracování tedy bylo považováno za a priori slučitelné, pokud existují jiné záruky a operace v zásadě vylučují použití získaných informací k rozhodnutím nebo opatřením týkajícím se konkrétního jednotlivce.

6.1.7. Automatizované individuální rozhodování, včetně profilování

Automatizovaná rozhodnutí jsou rozhodnutí přijatá za použití osobních údajů zpracovaných výlučně automatizovanými prostředky bez jakéhokoliv lidského zásahu. **Právo EU** stanoví, že subjekty údajů nesmějí být předmětem automatizovaných rozhodnutí, která mají právní nebo podobně významné účinky. Pokud je pravděpodobné, že tato rozhodnutí budou mít významný dopad na životy jednotlivců, jichž se týkají, například na jejich úvěruschopnost, elektronický nábor, pracovní výkon nebo analýzu chování či spolehlivosti, pak je nezbytná zvláštní ochrana, aby se předešlo negativním důsledkům. Automatické rozhodování zahrnuje profilování, jehož podstatou je jakákoliv forma automatizovaného hodnocení „osobní[ch] aspekt[ů] vztahující[ch] se k fyzické osobě, zejména za účelem analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu“.[606]

Příklad: Za účelem rychlého posouzení úvěruschopnosti budoucího zákazníka shromažďují agentury pro hodnocení úvěruschopnosti určité údaje o tom, jak zákazník využívá své úvěry a účty k hrazení veřejných a jiných služeb, podrobnosti o předchozích adresách zákazníka i informace z veřejných zdrojů, např. ze seznamu voličů, veřejných záznamů (včetně soudních rozhodnutí), nebo údaje o úpadku a platební neschopnosti. Tyto osobní údaje jsou následně posouzeny hodnotícím algoritmem, který vypočte celkovou hodnotu představující úvěruschopnost možného zákazníka.

Podle pracovní skupiny zřízené podle článku 29 právo nebýt předmětem rozhodnutí založených výlučně na automatizovaném zpracování, která mohou mít právní

606 Tamtéž, 71. bod odůvodnění, čl. 4 bod 4 a článek 22.

důsledky pro subjekt údajů nebo která ho mohou významně ovlivnit, znamená obecný zákaz a nevyžaduje, aby subjekt údajů aktivně proti takovému rozhodnutí vznášel námitku.[607]

Přesto podle GDPR může být automatizované rozhodování s právními účinky nebo takové, které se významným způsobem dotýká jednotlivců, přijatelné, pokud je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů nebo pokud k němu subjekt údajů udělí výslovný souhlas. Rovněž je automatizované rozhodování přípustné, pokud je povoleno právním řádem a pokud je vhodně zajištěna ochrana práv a svobod a oprávněných zájmů subjektu údajů.[608]

GDPR také stanoví, že mezi povinnosti správce, pokud jde o informace, jež je třeba poskytnout v případě shromažďování údajů, patří nutnost informovat subjekty údajů o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.[609] Právo na přístup k osobním údajům zpracovávaným správcem není dotčeno.[610] Informace by se neměly omezit pouze na skutečnost, že dochází k profilování, ale měly by také obsahovat smysluplné informace týkající se postupu použitého při profilování a předpokládané důsledky zpracování pro jednotlivce.[611] Například zdravotní pojišťovna používající automatické rozhodování při vyřizování žádostí by měla subjektům údajů poskytnout obecné informace o tom, jak fungují algoritmy a které faktory algoritmus používá k výpočtu pojistného. Obdobně při výkonu „práva na přístup" mohou subjekty údajů požádat správce o informace o skutečnosti, že dochází k automatizovanému rozhodování, a o smysluplné informace týkající se použitého postupu.[612]

Informace poskytnuté subjektům údajů mají zajistit transparentnost a umožnit jim udělit informovaný souhlas, je-li to nezbytné, nebo dosáhnout lidského zásahu. Správci údajů jsou povinni zavést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů. To zahrnuje alespoň práva dosáhnout lidského zásahu ze strany správce, a možnost, aby subjekt údajů vyjádřil svůj názor a mohl

607 Pracovní skupina zřízená podle článku 29, *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, WP 251, 3. října 2017, s. 15.

608 Obecné nařízení o ochraně osobních údajů, čl. 22 odst. 2.

609 Tamtéž, článek 12.

610 Tamtéž, článek 15.

611 Tamtéž, čl. 13 odst. 2 písm. f).

612 Tamtéž, čl. 15 odst. 1 písm. h).

napadnout rozhodnutí založené na automatizovaném zpracování jeho osobních údajů.[613]

Pracovní skupina zřízená podle článku 29 poskytla další pokyny k používání automatizovaného rozhodování v souladu s GDPR.[614]

Podle práva RE mají jednotlivci právo nebýt předmětem rozhodnutí, které pro ně má významný dopad a které je založeno výlučně na automatizovaném zpracování, aniž by byly zohledněny jejich názory.[615] Požadavek zvážit názory subjektu údajů v případě, že jsou rozhodnutí založena výlučně na automatizovaném zpracování, znamená, že subjekty údajů mají právo tato rozhodnutí napadnout a měly by být schopny rozporovat veškeré nepřesnosti v osobních údajích, které správce používá, napadnout i to, zda je na ně uplatněný profil relevantní.[616] Jednotlivec však nemůže toto právo uplatňovat, pokud je automatizované rozhodnutí povoleno zákonem, jímž se správce řídí a který také stanoví vhodná opatření, která zaručují práva, svobody a legitimní zájmy subjektu údajů. Kromě toho mají subjekty údajů právo na požádání získat informace o důvodech, na nichž je prováděné zpracování údajů založeno.[617] Ve Vysvětlující zprávě k Modernizované úmluvě č. 108 se uvádí příklad hodnocení pro poskytnutí úvěru. Jednotlivci by měli mít nárok se dozvědět nejen o samotných pozitivních či negativních rozhodnutích v oblasti hodnocení, ale též se seznámit s *obecnými principy*, kterými se zpracování jejich osobních údajů řídí a které vedly k přijetí tohoto rozhodnutí. „Porozumění těmto prvkům přispívá k účinnému výkonu jiných nezbytných záruk, jako je právo vznést námitku a právo podat stížnost příslušnému orgánu.“[618]

Doporučení o profilování, ačkoliv není právně závazné, upřesňuje podmínky pro shromažďování a zpracovávání osobních údajů v souvislosti s profilováním.[619] Obsahuje ustanovení o potřebě zajistit, že zpracování v souvislosti s profilováním by mělo být korektní, zákonné, přiměřené a za konkrétním a legitimním účelem. Rovněž zahrnuje ustanovení o informacích, které by měli správci poskytovat subjektům

613 Tamtéž, čl. 22 odst. 3.

614 Pracovní skupina zřízená podle článku 29 (2017), *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, WP 251, 3. října 2017.

615 Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. a).

616 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 75.

617 Modernizovaná úmluva č. 108, čl. 9 odst. 1 písm. c).

618 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 77.

619 Rada Evropy(2010): Doporučení CM/Rec(2010)13 Výboru ministrů členským státům o ochraně osob s ohledem na automatizované zpracování osobních údajů, článek 5.5.

údajů. Rovněž se v doporučení zmiňuje zásada kvality údajů – která ukládá správcům povinnost přijmout opatření k nápravě faktorů způsobujících nepřesnost údajů a k omezení rizika či chyb způsobených profilováním a povinnost pravidelně hodnotit kvalitu údajů a použitých algoritmů.

6.2. Právní ochrana, odpovědnost, pokuty a odškodnění

Hlavní body

- Podle Modernizované úmluvy č. 108 musí vnitrostátní právo smluvních stran stanovit vhodnou právní ochranu a postihy za porušení práva na ochranu údajů.
- V EU stanoví GDPR právní ochranu subjektů údajů v případě porušení jejich práv, jakož i postihy pro správce a zpracovatele, kteří jednají v souladu s ustanoveními tohoto nařízení. Rovněž stanoví právo na náhradu újmy a odpovědnost.
    - Subjekty údajů mají právo přímo podat stížnost u dozorového úřadu na údajné porušení nařízení a také mají právo na účinnou právní ochranu a na získání odškodnění.
    - Při výkonu svého práva na účinnou ochranu mohou být jednotlivci zastoupeni neziskovými organizacemi, které působí v oblasti ochrany údajů.
    - Správce nebo zpracovatel je odpovědný za hmotnou či nehmotnou újmu vzniklou v důsledku porušení předpisů.
    - Dozorové úřady mají pravomoc ukládat správní pokuty za porušení nařízení do výše až 20 000 000 EUR nebo v případě podniku do výše 4 % celkového celosvětového ročního obratu – podle toho, která částka je vyšší.
- Subjekty údajů mohou předložit případy porušení práva v oblasti ochrany údajů jako poslední možnost a po splnění určitých podmínek ESLP.
- Každá fyzická nebo právnická osoba má právo podat stížnost proti jakémukoliv rozhodnutí Evropského sboru pro ochranu osobních údajů u SDEU za podmínek stanovených ve Smlouvách.

Přijetí právních nástrojů nepostačuje k zajištění ochrany osobních údajů v Evropě. Aby byla evropská pravidla v oblasti ochrany údajů účinná, je nutné stanovit mechanismy, které umožní jednotlivcům zasazovat se proti porušování svých práv a usilovat o odškodnění za veškerou utrpěnou újmu. Rovněž je důležité, aby dozorové

úřady měly pravomoc ukládat postihy, které jsou účinné, odrazující a přiměřené danému případu porušení práva.

Práva podle právních předpisů v oblasti ochrany údajů může vykonávat osoba, jejíž práva jsou dotčena – bude se nejspíše jednat o osobu, která je subjektem těchto údajů. Avšak při výkonu práv mohou být subjekty údajů zastupovány i jinými osobami – pokud splňují nezbytné požadavky stanovené vnitrostátním právním řádem. Řada vnitrostátních právních řádů stanoví, že děti a osoby s mentálním postižením musí být zastoupeny jejich opatrovníky.[620] Podle evropského práva v oblasti ochrany údajů může subjekty údajů u dozorového úřadu nebo u soudu zastupovat sdružení – jehož zákonným cílem je podporovat práva v oblasti ochrany údajů.[621]

6.2.1. Právo podat stížnost u dozorového úřadu

Jednotlivci mají podle práva **RE** i **EU** právo, pokud se domnívají, že zpracování jejich osobních údajů neprobíhá v souladu s právními předpisy, podat žádosti a stížnosti u příslušného dozorového úřadu.

Modernizovaná úmluva č. 108 uznává právo subjektů údajů mít prospěch z pomoci dozorového úřadu při výkonu jejich práv podle úmluvy, a to bez ohledu na státní příslušnost a místo pobytu.[622] Žádost o pomoc lze zamítnout pouze za výjimečných okolností a subjekty údajů by neměly hradit náklady a poplatky spojené s touto pomocí.[623]

Podobná ustanovení lze nalézt v právním řádu EU. GDPR ukládá dozorovým úřadům povinnost přijmout opatření za účelem usnadnění podávání stížností, například vytvořením elektronického formuláře za tímto účelem.[624] Subjekt údajů může podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení.[625] Stížnosti musí

620 FRA (2015), Příručka evropského práva v oblasti práv dítěte, Lucemburk, Úřad pro publikace; FRA (2013), Právní způsobilost osob s mentálním postižením a osob s duševními poruchami, Lucemburk, Úřad pro publikace.

621 Obecné nařízení o ochraně osobních údajů, článek 80.

622 Modernizovaná úmluva č. 108, článek 18.

623 Tamtéž, články 16–17.

624 Obecné nařízení o ochraně osobních údajů, čl. 57 odst. 2.

625 Tamtéž, čl. 77 odst. 1.

být prošetřeny a dozorový úřad musí dotčenou osobu informovat o výsledku řízení vyřizujícího danou stížnost.[626]

Případná porušení předpisů ze strany orgánů a institucí EU mohou být předložena evropskému inspektorovi ochrany údajů.[627] Pokud EIOÚ do šesti měsíců neodpoví, považuje se stížnost za zamítnutou. Odvolání proti rozhodnutím EIOÚ lze podat k SDEU v rámci nařízení (ES) č. 45/2001, které stanoví orgánům a institucím EU povinnost řídit se pravidly v oblasti ochrany údajů.

Musí existovat možnost odvolat se proti rozhodnutím vnitrostátního dozorového úřadu k soudu. To se týká subjektů údajů i správců a zpracovatelů, kteří byli účastníky řízení u dozorového úřadu.

Příklad: V září 2017 uložil španělský orgán pro ochranu údajů pokutu společnosti Facebook za porušení několika nařízení v oblasti ochrany údajů. Dozorový úřad nesouhlasil s tím, že sociální síť shromažďovala, ukládala a zpracovávala osobní údaje, včetně zvláštních kategorií osobních údajů, pro účely reklamy, aniž by získala souhlas subjektu údajů. Rozhodnutí bylo založeno na vyšetřování provedeném z vlastní iniciativy dozorového úřadu.

6.2.2. Právo na účinnou soudní ochranu

Kromě práva podat stížnost u dozorového úřadu musí mít jednotlivci právo na účinnou soudní ochranu a právo obrátit se na soud. Právo na právní ochranu je řádně zakotveno v evropské právní tradici a je uznáváno jako jedno ze základních práv, a to jak podle článku 47 Listiny základních práv EU, tak podle článku 13 EÚLP.[628]

V rámci práva EU je význam poskytování účinné právní ochrany subjektům údajů v případech porušení jejich práv zjevný jak z ustanovení GDPR – které stanoví právo na účinnou soudní ochranu s ohledem na dozorové úřady, správce a zpracovatele –, tak z judikatury SDEU.

626 Tamtéž, čl. 77 odst. 2.

627 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

628 Viz například rozsudek ESLP ze dne 7. června 2016, *Karabeyoğlu v. Turecko*, č. 30083/10; rozsudek ESLP ze dne 18. července 2017, *Mustafa Sezgin Tanrıkulu v. Turecko*, č. 27473/06.

Příklad: Ve věci *Schrems*[629] prohlásil SDEU rozhodnutí o odpovídající ochraně („bezpečném přístavu“) za neplatné. Toto rozhodnutí umožnilo mezinárodní předávání údajů z EU organizacím v USA, které disponovaly vlastním osvědčením v rámci režimu „bezpečného přístavu“. SDEU se domníval, že režim „bezpečného přístavu“ má několik nedostatků, které ohrožují základní práva občanů EU na ochranu soukromí, ochranu osobních údajů a právo na účinnou právní ochranu.

Pokud jde o porušování práv na soukromí a na ochranu osobních údajů, SDEU zdůraznil, že právní předpisy USA umožňovaly některým veřejným orgánům přístup k osobním údajům předaným ze členských států do USA a jejich zpracování způsobem, který byl neslučitelný s účely, pro které byly původně předány, a nad rámec toho, co je přísně vzato nezbytné a přiměřené pro ochranu národní bezpečnosti. K právu na účinnou ochranu poznamenal, že subjekty údajů nemají k dispozici žádné správní nebo soudní prostředky, jež by umožňovaly zejména získat přístup k údajům, které se jich týkají, a případně dosáhnout jejich opravy nebo výmazu. SDEU dospěl k závěru, že právní úprava, která nestanoví žádnou možnost využít právních prostředků s cílem získat přístup k vlastním osobním údajům nebo dosáhnout opravy či výmazu těchto údajů, „nerespektuje podstatu základního práva na účinnou právní ochranu zakotveného v článku 47 Listiny“. Zdůraznil, že existence účinného soudního přezkumu zajišťujícího dodržování právních předpisů je inherentní součástí právního státu.

Jednotlivci, správci nebo zpracovatelé, kteří chtějí napadnout právně závazné rozhodnutí dozorového úřadu, se mohou obrátit na soud.[630] Pojem „rozhodnutí“ je třeba vykládat široce tak, že zahrnuje výkon vyšetřovacích, sankčních a povolovacích pravomocí dozorových úřadů, jakož i rozhodnutí stížnost odmítnout či zamítnout. Avšak rozhodnutí, která nejsou právně závazná, například stanoviska nebo doporučení, která dozorový úřad vydá, nemohou být předmětem žaloby u soudu.[631] Žaloba musí být podána u soudů členského státu, kde je usazen příslušný dozorový úřad.[632]

629 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

630 Obecné nařízení o ochraně osobních údajů, článek 78.

631 Tamtéž, 143. bod odůvodnění.

632 Tamtéž, čl. 78 odst. 3.

Ve věcech, kdy správce nebo zpracovatel poruší práva subjektu údajů, jsou subjekty údajů oprávněny podat stížnost soudu.[633] U řízení vedených proti správci nebo zpracovateli je zvlášť důležité, aby měli jednotlivci možnost rozhodnout se, kde žalobu podají. Mohou podat žalobu buď ve členském státě, v němž má daný správce nebo zpracovatel provozovnu, nebo ve členském státě, kde mají subjekty údajů své obvyklé bydliště.[634] Druhá uvedená možnost jednotlivcům značně usnadňuje výkon jejich práv, protože jim umožňuje podat žalobu ve státě, kde bydlí, a v rámci jim známé soudní příslušnosti. Pokud by soudy pro zahájení řízení proti správcům a zpracovatelům byly omezeny na členský stát, v němž mají správci a zpracovatelé provozovnu, subjekty údajů bydlící v jiných členských státech by byly odrazovány od podání žaloby, protože to by obnášelo cestování a další náklady a řízení by mohla být vedena v cizím jazyce a v rámci cizí soudní příslušnosti. Jediná výjimka se týká případů, kdy je správce nebo zpracovatel orgánem veřejné moci a zpracování se provádí v rámci výkonu jejich veřejné moci. V takovém případě jsou příslušné k podání žaloby pouze soudy ve státě, kde sídlí příslušný orgán veřejné moci.[635]

Ačkoliv ve většině případů budou věci týkající se pravidel v oblasti ochrany údajů rozhodnuty u soudů členských států, některé věci mohou být předloženy SDEU. První možností je situace, kdy subjekt údajů, správce, zpracovatel nebo dozorový úřad usiluje o prohlášení rozhodnutí EDPB za neplatné. Žaloba se však řídí podmínkami stanovenými v článku 263 SFEU, což znamená, že má-li být přípustná, musí tito jednotlivci a subjekty prokázat, že se jich rozhodnutí sboru bezprostředně a osobně dotýkají.

Druhá možnost se týká věcí, kdy protiprávně zpracovávají osobní údaje orgány a instituce EU. Ve věcech, kdy orgány EU porušují právo v oblasti ochrany údajů, mohou podat subjekty údajů žalobu přímo Tribunálu EU (Tribunál je součástí SDEU). Tribunál je v prvním stupni odpovědný za vyřizování stížností na porušení práva EU orgány EU. Je tedy možné u něho podávat stížnosti i na EIOÚ – což je instituce EU.[636]

> Příklad: Ve věci *Bavarian Lager*[637] požádala uvedená společnost Evropskou komisi, aby jí zpřístupnila úplný zápis ze zasedání konaného Komisí, které se údajně týkalo právních otázek, jež byly pro tuto společnost významné.

633 Tamtéž, článek 79.

634 Tamtéž, čl. 79 odst. 2.

635 Tamtéž.

636 Nařízení (ES) č. 45/2001, čl. 32 odst. 3.

637 Rozsudek SDEU (velkého senátu) z roku 2010, C-28/08 P, *Evropská komise v. The Bavarian Lager Co. Ltd.*

Komise žádost společnosti o přístup zamítla z důvodu převažujících zájmů v oblasti ochrany údajů.[638] Společnost Bavarian Lager podle článku 32 nařízení o ochraně údajů orgány EU podala na toto rozhodnutí stížnost u Soudu prvního stupně (předchůdce Tribunálu). Ve svém rozhodnutí (věc T-194/04, *The Bavarian Lager Co. Ltd v. Komise Evropských společenství*) Soud prvního stupně rozhodnutí Komise o zamítnutí žádosti o přístup zrušil. Evropská komise se proti tomuto rozhodnutí odvolala k SDEU.

SDEU (ve složení velkého senátu) vynesl rozsudek, v němž zamítl rozsudek Soudu prvního stupně a potvrdil zamítavé rozhodnutí Evropské komise ohledně zamítnutí žádosti o přístup k úplnému zápisu ze zasedání s cílem ochránit osobní údaje osob, které se zasedání zúčastnily. SDEU se domníval, že Komise jednala správně, když zamítla zveřejnění informací, a to vzhledem k tomu, že účastníci neudělili souhlas se zveřejněním svých osobních údajů. Kromě toho společnost Bavarian Lager neprokázala nezbytnost získání přístupu k těmto informacím.

V neposlední řadě mohou subjekty údajů, dozorové úřady, správci nebo zpracovatelé v průběhu vnitrostátních řízení požádat vnitrostátní soud, aby si vyžádal vyjasnění od SDEU ohledně výkladu a platnosti aktů orgánů, institucí a jiných subjektů EU. Tomuto objasnění se říká rozhodnutí o předběžné otázce. Nejedná se o přímou právní ochranu stěžovatele, ale umožňuje to vnitrostátním soudům zajistit, že vykládají právo EU náležitě. Pomocí mechanismu rozhodnutí o předběžné otázce se k SDEU dostaly zásadní věci – například *Digital Rights Ireland* a *Kärntner Landesregierung a další*[639] a *Schrems*[640] –, jež významně ovlivnily vývoj práva EU v oblasti ochrany údajů.

638 Analýzu argumentů naleznete zde: EIOÚ (2011), *Public access to documents containing personal data after the Bavarian Lager ruling* [Přístup veřejnosti k dokumentům obsahujícím osobní údaje v návaznosti na rozsudek ve věci Bavarian Lager], Brusel, EIOÚ.

639 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

640 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

Příklad: *Digital Rights Ireland* a *Kärntner Landesregierung a další*[641] byly spojené věci předložené irským vrchním soudem (High Court) a rakouským ústavním soudem, které se týkaly souladu směrnice 2006/24/ES (směrnice o uchovávání údajů) s právem EU v oblasti ochrany údajů. Rakouský ústavní soud předložil SDEU otázky týkající se platnosti článků 3 až 9 směrnice 2006/24/ES s ohledem na články 7, 9 a 11 Listiny základních práv EU. Mezi nimi byla i otázka, zda určitá ustanovení rakouského spolkového zákona o telekomunikacích, kterým se provádí směrnice o uchovávání údajů, nejsou neslučitelná s aspekty někdejší směrnice o ochraně údajů a nařízení o ochraně údajů orgány EU.

Ve věci *Kärntner Landesregierung a další* pan Seitlinger – jeden z navrhovatelů v řízení u ústavního soudu – tvrdil, že používal telefon, internet a e-mail k pracovním účelům i ve svém soukromém životě. Tudíž informace, které odesílal a přijímal, procházely veřejnými komunikačními sítěmi. Podle rakouského zákona o telekomunikacích z roku 2003 měl jeho poskytovatel telekomunikací zákonnou povinnost shromažďovat a ukládat údaje o tom, jak pan Seitlinger síť využívá. Pan Seitlinger se domníval, že toto shromažďování a ukládání jeho osobních údajů je pro technické účely odesílání a přijímání informací prostřednictvím sítě zbytečné. Shromažďování a ukládání těchto údajů pak nebylo skutečně nezbytné ani pro účely vyúčtování. Pan Seitlinger uvedl, že neudělil souhlas s používáním svých osobních údajů, které byly shromažďovány a ukládány výlučně podle rakouského zákona o telekomunikacích z roku 2003.

Podal tedy žalobu u rakouského ústavního soudu, v níž namítal, že zákonné povinnosti jeho poskytovatele telekomunikací byly v rozporu s jeho základními právy podle článku 8 Listiny základních práv EU. Vzhledem k tomu, že daný rakouský předpis provádí právo EU (tehdejší směrnici o uchovávání údajů), postoupil rakouský ústavní soud záležitost SDEU, aby rozhodl o slučitelnosti směrnice s právem na soukromí a ochranu údajů, které jsou zakotveny v Listině základních práv EU.

Velký senát SDEU o věci rozhodl a toto rozhodnutí mělo za následek zrušení směrnice EU o uchovávání údajů. SDEU shledal, že směrnice představovala zvlášť závažný zásah do základních práv na soukromí a ochranu údajů, aniž by

641 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

byl takový zásah přesně omezen na nezbytné minimum. Směrnice sledovala dosažení legitimních cílů, protože umožňovala vnitrostátním orgánům získat další příležitosti k vyšetřování a stíhání závažných trestných činů, a jednalo se tedy o cenný nástroj pro vyšetřování trestné činnosti. SDEU však konstatoval, že by se omezení základních práv měla použít pouze tehdy, pokud je to naprosto nezbytné, a měla by být doplněna o jasná a přesná pravidla pro rozsah a o dostatečné záruky pro jednotlivce.

Podle SDEU směrnice v této zkoušce nezbytnosti neobstála. Zaprvé, nestanovila jasná a přesná pravidla za účelem omezení rozsahu zásahu. Namísto toho, aby stanovila podmínku souvislosti mezi uchovávanými údaji a závažnou trestnou činností, vztahovala se směrnice na veškerá metadata všech uživatelů všech prostředků elektronické komunikace. Představovala tudíž zásah do práva na soukromí a práva na ochranu údajů prakticky celého obyvatelstva EU, což je možné považovat na nepřiměřené. Neobsahovala podmínky, které by omezily osoby oprávněné přistupovat k osobním údajům, ani nebyl tento přístup podmíněn procesními podmínkami, jako je požadavek na získání předběžného povolení k přístupu od správního orgánu nebo soudu. V neposlední řadě směrnice nestanovila jasné záruky pro ochranu uchovávaných údajů. Nedokázala tedy zajistit účinnou ochranu údajů před rizikem zneužití a před veškerým neoprávněným přistupováním k údajům a jejich protiprávním využíváním.[642]

V zásadě musí SDEU zodpovědět všechny postoupené otázky a nemůže odmítnout vynesení rozhodnutí o předběžné otázce z důvodů, že tato odpověď by nebyla relevantní ani včasná s ohledem na původní řízení. Může však odmítnout, pokud otázka nespadá do oblasti jeho působnosti.[643] SDEU vynáší rozhodnutí pouze ohledně základních prvků žádosti postoupené za účelem vydání rozhodnutí o předběžné otázce, zatímco vnitrostátnímu soudu i nadále přísluší rozhodnout v původní věci.[644]

Podle práva RE musejí smluvní strany stanovit vhodné soudní a mimosoudní ochranné prostředky pro případ porušení ustanovení Modernizované úmluvy

642 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, bod 69.

643 Rozsudek SDEU ze dne 16. prosince 1981, C-244/80, *Pasquale Foglia v. Mariella Novello (č. 2)*; rozsudek SDEU ze dne 28. září 2006, C-467/04, *Trestní řízení proti Giuseppe Francesco Gasparini a dalším*.

644 Rozsudek SDEU (velkého senátu) ze dne 11. prosince 2007, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union v. Viking Line ABP a OÜ Viking Line Eesti*, bod 85.

č. 108.[645] Žaloby na některou smluvní stranu EÚLP z důvodu údajného porušení práv v oblasti ochrany údajů v rozporu s článkem 8 EÚLP mohou být také předloženy ESLP po vyčerpání všech dostupných vnitrostátních opravných prostředků. Námitka porušení článku 8 EÚLP u ESLP musí splňovat také další kritéria přípustnosti (články 34–35 EÚLP).[646]

Ačkoliv podání k ESLP mohou být namířena pouze proti smluvním stranám, mohou se nepřímo týkat kroků nebo opomenutí soukromých stran, pokud smluvní strana nesplnila své pozitivní povinnosti podle EÚLP a nezajistila ve svém vnitrostátním právním řádu dostatečnou ochranu před porušováním práv v oblasti ochrany údajů.

Příklad: Ve věci *K.U. v. Finsko*[647] si stěžovatel – nezletilá osoba – stěžoval, že na internetové seznamce byl o něm zveřejněn inzerát sexuální povahy. Poskytovatel služby neodhalil totožnost osoby, která informace zveřejnila, kvůli povinnosti zachovávat služební tajemství, jíž stanoví finský právní řád. Stěžovatel namítal, že finské právo nestanovilo dostatečnou ochranu proti takovýmto krokům soukromé osoby, která umísťuje na internet inkriminující údaje o stěžovateli. ESLP rozhodl, že státy mají nejen povinnost zdržet se svévolného zasahování do soukromých životů jednotlivců, ale také mohou mít pozitivní povinnosti, k nimž patří „přijímání opatření k zajištění respektování soukromého života, a to i v oblasti vztahů jednotlivců mezi sebou navzájem". V případě stěžovatele bylo k jeho praktické a účinné ochraně nutné, aby byly přijaty účinné kroky k identifikaci a stíhání pachatele. Stát však tuto ochranu nezajistil a soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Köpke v. Německo*[648] byla stěžovatelka podezřívána z krádeže na svém pracovišti a podrobena skrytému sledování videokamerou. ESLP dospěl k závěru, že nic „nenasvědčovalo tomu, že vnitrostátní orgány nedosáhly spravedlivé rovnováhy v rámci svého prostoru pro vlastní rozhodování mezi právem stěžovatelky na respektování jejího soukromého života podle článku 8 a také zájmem jejího zaměstnavatele na ochraně jeho majetkových práv a veřejného zájmu při náležitém výkonu spravedlnosti". Stížnost byla proto prohlášena za nepřípustnou.

645 Modernizovaná úmluva č. 108, článek 12.

646 EÚLP, články 34–37.

647 Rozsudek ESLP ze dne 2. prosince 2008, *K.U. v. Finsko*, č. 2872/02.

648 Rozsudek ESLP ze dne 5. října 2010, *Köpke v. Německo* (dec.), č. 420/07.

Pokud ESLP dospěje k závěru, že smluvní strany porušily některé z práv stanovených EÚLP, je tato smluvní strana povinna vykonat rozsudek ESLP (článek 46 EÚLP). Opatření k vykonání rozsudku musí nejprve zastavit porušování a v rozsahu, v jakém je to možné, napravit negativní důsledky pro stěžovatele. Výkon rozsudků může také vyžadovat obecná opatření, která zabrání podobným případům porušení, jako jsou ty, které shledal soud, ať už prostřednictvím změny právních předpisů, judikaturou, nebo jinými nařízeními.

Pokud ESLP zjistí, že došlo k porušení EÚLP, stanoví článek 41 EÚLP, že může přiznat stěžovateli „spravedlivé zadostiučinění" na úkor dané smluvní strany.

Právo pověřit neziskový subjekt, organizaci nebo sdružení

GDPR umožňuje jednotlivcům podat stížnost u dozorového úřadu nebo žalobu u soudu a pověřit zastupováním neziskový subjekt, organizaci nebo sdružení.[649] Tyto neziskové subjekty musí mít statutární cíle, jež jsou ve veřejném zájmu, a vyvíjet činnost v oblasti ochrany údajů. Mohou jménem subjektu (subjektů) údajů podat stížnost nebo vykonávat právo na soudní ochranu. Nařízení uděluje členským státům možnost rozhodnout – v souladu s vnitrostátním právem –, zda může určitý subjekt podávat stížnosti jménem subjektů údajů, aniž by měl od nich zmocnění.

Toto právo na zastupování umožňuje jednotlivcům těžit z odborných znalostí a organizačních a finančních kapacit těchto neziskových subjektů, a tím významně jednotlivcům usnadňuje výkon jejich práv. GDPR těmto subjektům umožňuje podávat kolektivní žaloby jménem většího počtu subjektů údajů. To je rovněž ku prospěchu fungování a účinnosti soudního systému, protože se podobné nároky seskupí a přezkoumávají společně.

6.2.3. Odpovědnost a právo na náhradu

Právo na účinnou právní ochranu musí jednotlivce zmocňovat k tomu, aby žádali o náhradu za veškeré škody, které utrpí v důsledku zpracování svých osobních údajů způsobem, který je v rozporu s platnými právními předpisy. Odpovědnost správců a zpracovatelů za nezákonné zpracování je výslovně uznána v GDPR.[650] Nařízení přiznává jednotlivcům právo na získání náhrady od správce nebo zpracovatele za hmotnou i nehmotnou újmu, zatímco v bodech odůvodnění tohoto nařízení se uvádí,

649 Obecné nařízení o ochraně osobních údajů, článek 80.

650 Tamtéž, článek 82.

že „poj[em] „újma" by měl být široký a opírat se o judikaturu Soudního dvora při plném zohlednění cílů tohoto nařízení".[651] Správci nesou odpovědnost a mohou být povinni vyplatit náhradu v případě, že neplní své povinnosti stanovené nařízením. Zpracovatelé osobních údajů nesou odpovědnost za škodu způsobenou zpracováním pouze tehdy, pokud nejednali v souladu s povinnostmi stanovenými v tomto nařízení, které jsou výslovně určeny zpracovatelům, nebo pokud jednali nad rámec zákonných pokynů správce nebo v rozporu s nimi. Jestliže správce nebo zpracovatel zaplatil plnou náhradu, stanoví GDPR, že má právo žádat – od ostatních správců nebo zpracovatelů zapojených do téhož zpracování – vrácení části náhrady, která odpovídá jejich podílu na odpovědnosti za újmu.[652] Současně pak jsou výjimky z odpovědnosti velmi přísné a je třeba prokázat, že správce nebo zpracovatel není v žádném ohledu zodpovědný za událost, která vedla ke vzniku škody.

Náhrada musí být „plná a účinná" s ohledem na utrpěnou újmu. Pokud je újma způsobena zpracováním ze strany více správců a zpracovatelů, musí být každý správce nebo zpracovatel odpovědný za celou újmu. Cílem tohoto pravidla je zajistit účinnou náhradu subjektům údajů a koordinovaný přístup k dodržování předpisů ze strany správců a zpracovatelů zapojených do činností zpracování.

Příklad: Subjekty údajů nejsou povinny podat žalobu a požadovat náhradu od všech subjektů odpovědných za újmu, protože takováto situace by mohla zahrnovat nákladné a zdlouhavé řízení. Stačí podat žalobu na jednoho ze společných správců, který může pak nést odpovědnost za plnou výši škody. V takovýchto případech správce nebo zpracovatel, který zaplatí náhradu, je následně oprávněn získat vyplacenou částku zpět od ostatních subjektů zapojených do zpracování a odpovědných za porušení předpisů, a to za jejich podíl na odpovědnosti za škodu. Tato řízení mezi jednotlivými společnými správci a zpracovateli probíhají poté, co subjekt údajů obdržel náhradu škody, a subjekt údajů není jejich účastníkem.

V právním rámci RE ukládá článek 12 Modernizované úmluvy č. 108 smluvním stranám povinnost stanovit vhodné opravné prostředky pro případ porušení ustanovení vnitrostátního práva provádějícího požadavky úmluvy. Ve Vysvětlující zprávě k Modernizované úmluvě č. 108 se uvádí, že opravné prostředky musí zahrnovat možnost soudně napadnout rozhodnutí nebo postup a že současně musí být

651 Tamtéž, 146. bod odůvodnění.

652 Tamtéž, čl. 82 odst. 2 a 5.

k dispozici také mimosoudní prostředky.[653] Různé formy a pravidla související s přístupem k těmto opravným prostředkům, jakož i postupy, které je třeba dodržet, jsou ponechány na uvážení každé smluvní strany. Smluvní strany a vnitrostátní soudy mohou také zvážit ustanovení o finanční náhradě za hmotnou a nehmotnou újmu způsobenou zpracováním, jakož i možnost umožnit podání kolektivních žalob.[654]

6.2.4. Sankce

V rámci práva RE stanoví článek 12 Modernizované úmluvy č. 108, že každá smluvní strana musí stanovit vhodné postihy a opravné prostředky pro případ porušení ustanovení vnitrostátního práva uplatňujícího základní zásady ochrany údajů uvedené v úmluvě č. 108. Úmluva nestanoví ani neukládá nějaký konkrétní soubor sankcí. Naopak. Jasně uvádí, že každá smluvní strana může volně určit povahu soudních a mimosoudních sankcí, které mohou být trestněprávní, správní nebo občanskoprávní. Vysvětlující zpráva k Modernizované úmluvě č. 108 stanoví, že sankce musí být účinné, přiměřené a odrazující.[655] Smluvní strany musejí tuto zásadu respektovat při určování povahy a závažnosti sankcí, které mají k dispozici ve svém vnitrostátním právním řádu.

V rámci práva EU zmocňuje článek 83 GDPR dozorové úřady členských států k ukládání správních pokut za porušení tohoto nařízení. Výše pokut a okolnosti, které vnitrostátní orgány zohledňují při rozhodování o uložení pokuty, jakož i celková maximální možná výše pokuty jsou také stanoveny v článku 83. Režim udělování sankcí je tedy v celé EU harmonizovaný.

GDPR se řídí odstupňovaným přístupem k pokutám. Dozorové úřady mají pravomoc ukládat správní pokuty za porušení nařízení do výše až 20 000 000 EUR nebo v případě podniku do výše 4 % jeho celkového celosvětového ročního obratu – podle toho, která částka je vyšší. Mezi případy porušení předpisů, které mohou vést k takovéto výši pokuty, patří porušení základních zásad zpracování a podmínek udělení souhlasu, porušení práv subjektů údajů a ustanovení nařízení, která upravují předávání osobních údajů příjemcům ve třetích zemích. Za jiné případy porušení předpisů mohou dozorové úřady uložit pokuty do výše až 10 000 000 EUR nebo v případě podniku do výše dvou procent jeho celkového celosvětového ročního obratu – podle toho, která částka je vyšší.

653 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 100.

654 Tamtéž.

655 Tamtéž.

Při určování druhu a výše pokuty, která má být uložena, musí dozorové úřady zohlednit řadu faktorů.[656] Musejí například řádně zohlednit povahu, závažnost a délku trvání porušení, dotčené kategorie osobních údajů a to, zda bylo porušení způsobeno úmyslně nebo z nedbalosti. Rovněž je třeba zohlednit, zda správce nebo zpracovatel přijal opatření ke zmírnění škody, kterou utrpěly subjekty údajů. Podobně jsou dalšími důležitými faktory, které slouží dozorovým úřadům jako vodítko při rozhodování, míra spolupráce s dozorovým úřadem poté, co dojde k porušení, a způsob, jakým se dozorový úřad o porušení dozvěděl (například zda je oznámil subjekt odpovědný za zpracování nebo subjekt údajů, jehož práva byla porušena).[657]

Vedle schopnosti ukládat správní pokyny mají dozorové úřady k dispozici širokou škálu jiných nápravných pravomocí. Takzvané „nápravné" pravomoci dozorových úřadů jsou uvedeny v článku 58 GDPR. Patří k nim vše od vydávání příkazů, upozornění a napomenutí správcům a zpracovatelům po ukládání dočasného, nebo dokonce trvalého zákazu provádění činností zpracování.

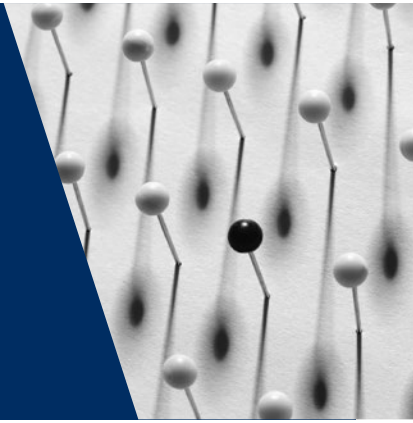
Pokud jde o sankce za porušení práva EU ze strany orgánů a institucí EU s ohledem na zvláštní oblast působnosti nařízení o ochraně údajů orgány EU, je možné stanovit sankce ve formě disciplinárních postihů. Článek 49 uvedeného nařízení stanoví, že „[j]akékoli porušení povinností vyplývajících z tohoto nařízení, ať úmyslné nebo z nedbalosti, vystavuje úředníky nebo ostatní zaměstnance Evropských společenství disciplinárním postihům […]".

656 Obecné nařízení o ochraně osobních údajů, čl. 83 odst. 2.

657 Pracovní skupina zřízená podle článku 29 (2017), *Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679*, WP 253, 3. října 2017.

7

Mezinárodní předávání údajů a toky osobních údajů



EU	Pojednávaná témata	RE
Předávání osobních údajů		
Obecné nařízení o ochraně osobních údajů, článek 44	Pojetí	Modernizovaná úmluva č. 108, čl. 14 odst. 1 a 2
Volný pohyb osobních údajů		
Obecné nařízení o ochraně osobních údajů, čl. 1 odst. 3 a 170. bod odůvodnění	Mezi členskými státy EU	
	Mezi smluvními stranami úmluvy č. 108	Modernizovaná úmluva č. 108, čl. 14 odst. 1
Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím		
Obecné nařízení o ochraně osobních údajů, článek 45 Rozsudek SDEU (velkého senátu) z roku 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*	Rozhodnutí o odpovídající ochraně / třetí země nebo mezinárodní organizace s odpovídající úrovní ochrany	Modernizovaná úmluva č. 108, čl. 14 odst. 2
Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 1 a čl. 46 odst. 2	Vhodné záruky, včetně vymahatelných práv a právní ochrany pro subjekty údajů, poskytnuté prostřednictvím smluvních doložek, závazných podnikových pravidel, kodexů chování a mechanismů pro vydávání osvědčení	Modernizovaná úmluva č. 108, čl. 14 odst. 2, 3, 5 a 6

EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 3	V závislosti na povolení od příslušného dozorového úřadu: smluvní doložky a ustanovení obsažená ve správních ujednáních mezi orgány veřejné moci	
Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 5	Stávající povolení na základě směrnice 95/46/ES	
Obecné nařízení o ochraně osobních údajů, článek 47	Závazná podniková pravidla	
Obecné nařízení o ochraně osobních údajů, článek 49	Výjimky pro zvláštní situace	Modernizovaná úmluva č. 108, čl. 14 odst. 4
Příklady: Dohoda EU–USA o jmenné evidenci cestujících Dohoda EU–USA o Společnosti pro celosvětovou mezibankovní finanční komunikaci (dohoda o SWIFT)	Mezinárodní dohody	Modernizovaná úmluva č. 108, čl. 14 odst. 3 písm. a)

V rámci práva EU stanoví obecné nařízení o ochraně osobních údajů volný pohyb údajů v rámci Evropské unie. Obsahuje však konkrétní povinnosti týkající se předávání osobních údajů do třetích zemí mimo EU a mezinárodním organizacím. Nařízení uznává význam těchto předávání, zejména s ohledem na mezinárodní obchod a spolupráci, ale také uznává zvýšená rizika pro osobní údaje. Cílem nařízení je proto nabídnout osobním údajů předávaným do třetích zemí stejnou úroveň ochrany, jaké se těší v EU.[658] Právo RE rovněž uznává význam prováděcích pravidel pro přeshraniční pohyby údajů na základě volného pohybu mezi stranami a zvláštních požadavků pro předávání státům, které nejsou smluvními stranami.

7.1. Charakter předání osobních údajů

Hlavní body

- Právní předpisy EU i RE obsahují pravidla pro předávání osobních údajů příjemcům ve třetích zemích nebo mezinárodním organizacím.
- Zabezpečení práv subjektů údajů při předávání údajů mimo EU umožňuje, aby si osobní údaje pocházející z EU zachovaly ochranu poskytovanou podle práva EU.

658 Obecné nařízení o ochraně osobních údajů, 101. a 116. bod odůvodnění.

V rámci **práva RE** jsou přeshraniční pohyby údajů popsány jako předání osobních údajů příjemcům, kteří mají zahraniční soudní příslušnost.[659] Přeshraniční pohyby údajů směrem k příjemci, který nemá soudní příslušnost některé smluvní strany, jsou povoleny pouze tehdy, pokud existuje vhodná úroveň ochrany.[660]

Právo EU upravuje předávání „osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci […]".[661] Tyto pohyby údajů jsou povoleny pouze tehdy, pokud jsou v souladu s pravidly stanovenými v kapitole V GDPR.

Přeshraniční pohyby osobních údajů jsou povoleny, pokud příjemce má soudní příslušnost některé smluvní strany podle práva RE nebo členského státu podle práva EU. Oba právní řády rovněž umožňují předávání údajů do země, která není smluvní stranou ani členským státem, pokud jsou splněny určité podmínky.

7.2. Volný pohyb/tok osobních údajů mezi členskými státy nebo smluvními stranami

Hlavní body

- Pohyb osobních údajů v rámci EU i předávání osobních údajů mezi smluvními stranami Modernizované úmluvy č. 108 nesmí být omezován. Jelikož však ne všechny smluvní strany Modernizované úmluvy č. 108 jsou členskými státy EU, předávání z členského státu EU do třetí země, která však je smluvní stranou Úmluvy č. 108, není možné, pokud nejsou splněny podmínky stanovené v nařízení GDPR.

Podle práva RE musí existovat volný pohyb osobních údajů mezi smluvními stranami Modernizované úmluvy č. 108. Předání však může být zakázáno, pokud existuje „skutečné a vážné riziko, že přenosem k jiné smluvní straně by došlo k obcházení ustanovení Úmluvy" nebo pokud je strana povinna tak učinit na základě „harmonizovaný[ch] pravid[el] ochrany, kter[á] jsou sdílen[a] státy náležejícími k regionální mezinárodní organizaci".[662]

659 Vysvětlující zpráva k Modernizované úmluvě č. 108, bod 102.

660 Modernizovaná úmluva č. 108, čl. 14 odst. 2.

661 Obecné nařízení o ochraně osobních údajů, článek 44.

662 Modernizovaná úmluva č. 108, čl. 14 odst. 1.

Podle práva EU[663] jsou omezení nebo zákaz volného pohybu osobních údajů mezi členskými státy EU z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů zakázány. Oblast volného pohybu údajů byla rozšířena Dohodou o Evropském hospodářském prostoru (EHP)[664], kterou se Island, Lichtenštejnsko a Norsko stávají součástí vnitřního trhu.

Příklad: Pokud dceřiná společnost mezinárodní skupiny společností, která je usazena v několika členských státech, mezi něž patří mimo jiné Slovinsko a Francie, zasílá osobní údaje ze Slovinska do Francie, nesmí být tento pohyb údajů omezen ani zakázán slovinským vnitrostátním právním řádem z důvodů spojených s ochranou osobních údajů.

Pokud však tatáž slovinská dceřiná společnost chce předávat tytéž osobní údaje mateřské společnosti v Malajsii, pak musí slovinský vývozce údajů zohlednit pravidla uvedená v kapitole V GDPR. Tato ustanovení mají za cíl ochránit osobní údaje subjektů údajů, které mají soudní příslušnost EU.

Podle práva EU se pohyby osobních údajů do členských států EHP za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů řídí směrnicí 2016/680.[665] To také zajišťuje, aby nebyla omezována nebo zakazována výměna osobních údajů příslušnými orgány v rámci Unie. Podle práva RE spadá do působnosti Úmluvy č. 108 zpracování všech osobních údajů (včetně přeshraničního pohybu s jinými stranami Úmluvy č. 108), bez výjimek založených na účelech nebo oblastech činnosti, ačkoliv smluvní strany mohou stanovit výjimky. Všichni členové EHP jsou také smluvními stranami Úmluvy č. 108.

663 Obecné nařízení o ochraně osobních údajů, čl. 1 odst. 3.

664 Rozhodnutí Rady a Komise ze dne 13. prosince 1993 o uzavření Dohody o Evropském hospodářském prostoru mezi Evropskými společenstvími, jejich členskými státy a Rakouskou republikou, Finskou republikou, Islandskou republikou, Lichtenštejnským knížectvím, Norským královstvím, Švédským královstvím a Švýcarskou konfederací, Úř. věst. 1994 L 1.

665 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, Úř. věst. 2016 L 119.

7.3. Předávání osobních údajů třetím zemím / zemím, které nejsou smluvními stranami, nebo mezinárodním organizacím

Hlavní body

- **RE** i **EU** umožňují předávání osobních údajů třetím zemím nebo mezinárodním organizacím, pokud jsou splněny určité podmínky pro ochranu osobních údajů.
  - **Podle práva RE** je možné dosáhnout odpovídající úroveň ochrany právními předpisy státu nebo mezinárodní organizace nebo zavedením odpovídajících norem.
  - **Podle práva EU** může předávání proběhnout, pokud třetí země zajišťuje odpovídající úroveň ochrany nebo pokud správce údajů nebo zpracovatel stanoví vhodné záruky, včetně vymahatelnosti práv subjektu údajů a právní ochrany, prostřednictvím prostředků, jako jsou standardní doložky o ochraně osobních údajů nebo závazná podniková pravidla.
- **Právo RE i právo EU** umožňují ustanovení o odchylkách, díky nimž je možné předávat osobní údaje za určitých okolností i tehdy, když není zajištěna odpovídající úroveň ochrany ani odpovídající záruky.

Ačkoliv právo RE i EU umožňují pohyb údajů směrem ke třetím stranám nebo mezinárodním organizacím, oba právní systémy stanoví odlišné podmínky. Každý soubor podmínek zohledňuje odlišnou strukturu a účely obou organizací.

Podle **práva EU** existují v zásadě dva způsoby, které umožňují předávání osobních údajů třetím zemím nebo mezinárodním organizacím. K předávání osobních údajů může dojít na základě: rozhodnutí Evropské komise o odpovídající ochraně;[666] nebo pokud takové rozhodnutí nebylo vydáno, zda správce nebo zpracovatel poskytuje vhodné záruky, včetně vymahatelných práv a prostředků právní ochrany pro subjekty údajů.[667] V případě, že nebylo vydáno rozhodnutí o odpovídající ochraně ani nebyly zavedeny vhodné záruky, je k dispozici řada výjimek.

Podle práva **RE** je však volné předávání údajů do zemí, které nejsou stranami úmluvy, možné pouze na základě:

666 Obecné nařízení o ochraně osobních údajů, článek 45.

667 Tamtéž, článek 46.

- právních předpisů daného státu nebo mezinárodní organizace, včetně platných mezinárodních smluv a dohod zaručujících odpovídající záruky,

- ad hoc nebo schválenými normalizovanými zárukami poskytovanými právně závaznými a vynutitelnými nástroji přijatými a prováděnými osobami zapojenými do předávání a dalšího zpracovávání.[668]

Podobně i v právu EU je v případě absence odpovídající úrovně ochrany údajů k dispozici řada výjimek.

7.3.1. Předávání na základě rozhodnutí o odpovídající ochraně

V rámci práva EU stanoví volný pohyb osobních údajů do třetích zemí s odpovídající úrovní ochrany údajů článek 45 GDPR. SDEU vyjasnil, že pojem „odpovídající úroveň ochrany" vyžaduje, aby třetí země zajišťovala úroveň ochrany základních práv a svobod, která je „v zásadě rovnocenná"[669] zárukám poskytnutým právním řádem v EU. Současně se prostředky, které třetí země využívá k zajištění takovéto úrovně ochrany, mohou lišit od prostředků zavedených v rámci EU; norma týkající se odpovídající ochrany nevyžaduje naprosto shodnou replikaci pravidel EU.[670]

Evropská komise posuzuje úroveň ochrany údajů v cizích zemích tím, že prozkoumá jejich vnitrostátní právo a příslušné mezinárodní závazky. Rovněž je třeba zohlednit zapojení určité země do multilaterálních nebo regionálních systémů, zejména s ohledem na ochranu osobních údajů. Pokud Evropská komise shledá, že daná třetí země nebo organizace zajišťuje odpovídající úroveň ochrany, může vydat rozhodnutí o odpovídající ochraně, které má závazný účinek.[671] SDEU přesto konstatoval, že vnitrostátní dozorové orgány stále mají pravomoc posoudit žádost osoby týkající se ochrany jejích osobních údajů, které byly předány do třetí země, již Komise považuje

668 Modernizovaná úmluva č. 108, čl. 14 odst. 3 písm. a) a b).

669 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, bod 96.

670 Tamtéž, bod 74. Viz také Evropská komise (2017´), Sdělení Komise Evropskému parlamentu a Radě „Výměna a ochrana osobních údajů v globalizovaném světě", COM(2017)7 final ze dne 10. ledna 2017, s. 6.

671 Soustavně aktualizovaný seznam zemí, které byly shledány jako země s odpovídající úrovní ochrany, lze nalézt na domovské stránce Evropské komise, Generálního ředitelství pro spravedlnost.

za zemi, která zajišťuje odpovídající úroveň ochrany, pokud tato osoba tvrdí, že právo a praxe platné v této zemi nezajišťují odpovídající úroveň ochrany.[672]

Evropská komise může také posoudit odpovídající úroveň ochrany určitého území v rámci třetí země nebo se omezit na určitá odvětví, jak tomu bylo například v případě kanadského právního předpisu o soukromém podnikání.[673] Byly rovněž vyvozeny závěry o odpovídající ochraně u převodů založených na dohodách mezi EU a třetími zeměmi. Tato rozhodnutí se týkají výlučně jednoho druhu předávání údajů, například předávání jmenné evidence cestujících (PNR) ze strany leteckého dopravce zahraničním orgánům pro ostrahu hranic v případě, že letecký dopravce provozuje dopravu z EU do určitých zahraničních destinací (viz oddíl 7.3.4).

Rozhodnutí o odpovídající ochraně jsou průběžně monitorována. Evropská komise pravidelně tato rozhodnutí přezkoumává s cílem sledovat vývoj, který by mohl ovlivnit jejich status. Tudíž pokud Evropská komise shledá, že daná třetí země nebo mezinárodní organizace již nesplňuje podmínky odůvodňující vydání rozhodnutí o odpovídající ochraně, může toto rozhodnutí změnit, pozastavit jeho platnost nebo je zrušit. Komise může rovněž zahájit vyjednávání se třetí zemí nebo dotčenou mezinárodní organizací s cílem napravit problém, který je příčinou jejího rozhodnutí.

Rozhodnutí o odpovídající ochraně přijatá Evropskou komisí na základě směrnice 95/46/ES zůstávají v platnosti do doby, než budou změněna, nahrazena nebo zrušena rozhodnutím Komise přijatým v souladu s pravidly podle článku 45 GDPR.

K dnešnímu dni Evropská komise uznala za země zajišťující odpovídající ochranu tyto státy: Andorra, Argentina, Kanada (obchodní organizace spadající do působnosti zákona o ochraně osobních informací a elektronických dokumentech – PIPEDA, Faerské ostrovy, Guernsey, Ostrov Man, Izrael, Jersey, Nový Zéland, Švýcarsko a Uruguay). Pokud jde o předávání údajů do USA, Evropská komise přijala rozhodnutí o odpovídající ochraně v roce 2000, které umožňovalo předávání údajů společnostem, které disponovaly vlastním osvědčením o tom, že chrání osobní údaje

672 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, body 63 a 65– 66.

673 Evropská komise (2002), Rozhodnutí ze dne 20. prosince 2001 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech (Personal Information Protection and Electronic Documents Act), Úř. věst. 2002 L 2.

předávané z EU a jednají v souladu s takzvanými „zásadami bezpečného přístavu“.[674] SDEU toto rozhodnutí v roce 2015 zrušil a nové rozhodnutí o odpovídající ochraně bylo přijato v červenci 2016. Toto rozhodnutí umožňovalo společnostem připojit se od 1. srpna 2016.

Příklad: Ve věci *Schrems*[675] rakouský občan Maximilian Schrems byl několik let uživatelem Facebooku. Některé nebo všechny údaje, které pan Schrems Facebooku poskytl, byly předány z irské pobočky Facebooku serverům nacházejícím se v USA, kde byly údaje zpracovány. Pan Schrems podal stížnost u irského orgánu na ochranu údajů s námitkou, že vzhledem k odhalením, která učinil americký whistleblower Edward Snowden ohledně sledovacích činností amerických zpravodajských služeb, nenabízí právo a praxe v USA dostatečnou ochranu údajů předaných do této země. Irský orgán stížnost zamítl z důvodu, že ve svém rozhodnutí ze dne 26. července 2000 se Komise domnívala, že v rámci režimu „bezpečného přístavu“ zajišťují USA dostatečnou úroveň ochrany předaných osobních údajů. Věc byla předložena irskému vrchnímu soudu (High Court), který ji postoupil SDEU, aby rozhodl o předběžné otázce.

SDEU rozhodl, že rozhodnutí Komise o odpovídající ochraně v rámci „bezpečného přístavu“ bylo neplatné. SDEU nejprve konstatoval, že rozhodnutí umožnilo omezit uplatnění zásad „bezpečného přístavu“ pro ochranu údajů na základě národní bezpečnosti, veřejného zájmu nebo prosazování zákonů nebo na základě vnitrostátních právních předpisů USA. Rozhodnutí proto umožnilo zasahovat do základních práv těch osob, jejichž osobní údaje byly nebo by mohly být předány do USA.[676] Dále konstatoval, že rozhodnutí neobsahuje žádný nález ohledně existence pravidel ve Spojených státech, jež mají omezit takové zásahy, ani ohledně existenci účinné právní ochrany před zásahy tohoto druhu.[677] SDEU zdůraznil, že úroveň ochrany základních práv a svobod zaručená v rámci EU vyžaduje, aby unijní právní předpisy zasahující

674 Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států, Úř. věst. L 215. Rozhodnutí prohlásil SDEU za neplatné v rozsudku (velkého senátu) ve věci C-632/14, *Maximillian Schrems v. Data Protection Commissioner*.

675 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

676 Tamtéž, bod 84.

677 Tamtéž, body 88–89.

do působnosti článků 7 a 8 stanovily jasná a přesná pravidla vymezující rozsah a použití dotčeného opatření a aby stanovily minimální záruky, výjimky z ochrany osobních údajů a její omezení.[678] Vzhledem k tomu, že v rozhodnutí Komise se neuvádělo, že USA skutečně zajišťují na základě svých vnitrostátních předpisů nebo mezinárodních závazků takovou úroveň ochrany, dospěl SDEU k závěru, že rozhodnutí nesplňuje požadavky příslušného ustanovení o předávání uvedeného ve směrnici o ochraně údajů, a je tudíž neplatné.[679]

Úroveň ochrany v USA tudíž nebyla „v zásadě rovnocenná" s ohledem na základní práva a svobody zaručené EU.[680] SDEU argumentoval tím, že byly porušeny různé články Listiny základních práv EU. Zaprvé bylo zasaženo do podstaty článku 7, protože právní předpisy USA „veřejným orgánům umožňuj[í] globální přístup k obsahu elektronických komunikací". Zadruhé byla porušena podstata článku 47, protože právní předpisy nedávaly jednotlivcům možnost využít právních prostředků s cílem získat přístup k osobním údajům nebo dosáhnout opravy či výmazu těchto údajů. Zatřetí osobní údaje již nebyly zpracovávány zákonně, protože dohoda o „bezpečném přístavu" byla v rozporu s výše uvedenými články, což mělo za následek porušení článku 8.

Poté, co SDEU prohlásil ujednání o „bezpečném přístavu" za neplatné, dohodly se Komise a USA na novém rámci, štítu EU–USA na ochranu soukromí. Dne 12. července 2016 přijala Komise rozhodnutí, ve kterém prohlásila, že USA zaručují odpovídající úroveň ochrany osobních údajů předávaných z Unie organizacím v USA v rámci režimu štítu na ochranu soukromí.[681]

Podobně jako v rámci ustanovení o „bezpečném přístavu" je cílem štítu EU–USA na ochranu soukromí ochránit osobní údaje, které jsou předávány z EU do USA za

678 Tamtéž, body 91–92.

679 Tamtéž, body 96–97.

680 Tamtéž, body 73–74 a 96.

681 Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí, Úř. věst. L 207. Pracovní skupina zřízená podle článku 29 uvítala zlepšení, která přinesl mechanismus štítu na ochranu soukromí ve srovnání s rozhodnutím o „bezpečném přístavu", a pochválila Komisi a orgány USA za to, že zohlednily v konečném znění dokumentů o štítu na ochranu soukromí obavy, které skupina vyjádřila ve svém stanovisku QP238 o předloze rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí. Přesto však zdůraznila řadu přetrvávajících obav. Pro více podrobností viz pracovní skupina pro ochranu údajů zřízená podle článku 29, *Stanovisko 01/2016 k předloze rozhodnutí o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí*, přijato dne 13. dubna 2016, 16/EN WP 238.

obchodními účely.[682] Společnosti v USA mohou dobrovolně samy osvědčit to, že jednají v souladu se seznamem organizací štítu na ochranu soukromí, tím, že se zaváží plnit normy ochrany údajů podle tohoto rámce. Příslušné orgány USA monitorují a ověřují, zda certifikované společnosti tyto normy splňují.

Režim štítu na ochranu soukromí zejména stanoví:

- povinnost společností přijímajících osobní údaje z EU zajišťovat ochranu údajů,
- ochranu a možnosti nápravy pro jednotlivce, zejména zřízení mechanismu ombudsmana, který je nezávislý na zpravodajských službách USA a vyřizuje stížnosti jednotlivců, kteří jsou přesvědčeni, že jejich osobní údaje byly orgány USA v oblasti národní bezpečnosti použity nezákonně,
- výroční společný přezkum s cílem monitorovat provádění rámce.[683] První přezkum proběhl v září 2017.[684]

Vláda USA sepsala závazky a záruky, které rozhodnutí o štítu na ochranu soukromí doplňují. Tyto závazky stanoví omezení a záruky pro přístup vlády USA k osobním údajům pro účely prosazování práva a národní bezpečnosti.

7.3.2. Předání na základě vhodných záruk

Podle **práva EU** i **práva RE** jsou uznávány vhodné záruky mezi správcem vyvážejícím údaje a příjemcem ve třetí zemi nebo mezinárodní organizaci jakožto možný prostředek pro zajištění odpovídající úrovně ochrany údajů na straně příjemce.

Právo EU stanoví, že předávání osobních údajů třetí zemi nebo mezinárodní organizaci je povoleno, pokud správce nebo zpracovatel stanoví vhodné záruky a vymahatelná práva a jestliže je subjektům údajů k dispozici účinná právní ochrana.[685] Seznam přijatelných „vhodných záruk" je stanoven výlučně v právu EU v oblasti ochrany údajů. Vhodné záruky je možné zajistit prostřednictvím:

682 Pro více informací viz informativní přehled o štítu EU–USA na ochranu soukromí.

683 Pro více informací viz webové stránky Evropské komise na adrese Štít EU–USA na ochranu soukromí.

684 Evropská komise, Zpráva Komise Evropskému parlamentu a Radě o prvním každoročním přezkumu fungování štítu EU–USA na ochranu soukromí, COM(2017) 611 final, 18. října 2017. Viz také pracovní skupina zřízená podle článku 29, *EU – U.S. Privacy Shield – First annual Joint Review* [Štít EU–USA na ochranu soukromí – první výroční společný přezkum], přijato dne 28. listopadu 2017, 17/EN WP 255.

685 Obecné nařízení o ochraně osobních údajů, článek 46.

- právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty,
- závazných podnikových pravidel,
- standardních doložek o ochraně osobních údajů přijatých buď Evropskou komisí, nebo dozorovým úřadem,
- kodexů chování,
- mechanismu pro vydání osvědčení.[686]

Na míru upravená smluvní ustanovení mezi správcem či zpracovatelem v EU a příjemcem údajů ve třetí zemi jsou další možnost, jak zajistit vhodné záruky. Tato smluvní ustanovení však musí být schválena příslušným dozorovým úřadem, než bude možné se na ně odvolávat jako na nástroj pro předávání osobních údajů. Obdobně mohou orgány veřejné moci využít ustanovení o ochraně údajů vložená do jejich správních ujednání, pokud jsou povolena dozorovým úřadem.[687]

Právo RE stanoví, že toky údajů do státu nebo mezinárodní organizace, která není stranou Modernizované úmluvy č. 108, jsou povoleny, pokud je zajištěna odpovídající úroveň ochrany. Toho lze dosáhnout prostřednictvím:

- zákona daného státu nebo mezinárodní organizace nebo
- ad hoc a standardizovanými zárukami zakotvenými v právně závazném dokumentu.[688]

Předání na základě smluvních doložek

Podle **práva RE** i **práva EU** jsou uznávány smluvní doložky mezi správcem vyvážejícím údaje a příjemcem ve třetí zemi jakožto možný prostředek pro zajištění odpovídající úrovně ochrany údajů na straně příjemce.[689]

686 Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 1 písm. c) a d), odst. 2 písm. a), b), e) a f) a článek 47.

687 Tamtéž, čl. 46 odst. 3.

688 Modernizovaná úmluva č. 108, čl. 14 odst. 3 písm. b).

689 Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 3, Modernizovaná úmluva č. 108, čl. 14 odst. 3 písm. b).

Na úrovni EU vypracovala Evropská komise za pomoci pracovní skupiny zřízené podle článku 29 standardní doložky o ochraně osobních údajů, které Komise úředně certifikovala jako důkaz o odpovídající ochraně údajů.[690] Jelikož rozhodnutí Komise jsou v členských státech závazná v celém rozsahu, musejí vnitrostátní orgány, které dohlížejí na předávání údajů, tyto standardní smluvní doložky uznávat v rámci svých postupů.[691] Pokud se tedy správce vyvážející údaje a příjemce ve třetí zemi dohodnou na těchto doložkách a stvrdí dohodu podpisem, měla by představovat pro dozorový úřad dostatečný důkaz, že jsou zavedeny vhodné záruky. Přesto však ve věci *Schrems* SDEU rozhodl, že Evropská komise nemá pravomoc omezit pravomoci vnitrostátních dozorových úřadů v oblasti dozoru nad předáváním osobních údajů do třetí země, které je založeno na rozhodnutí Komise o odpovídající ochraně.[692] Vnitrostátním dozorovým úřadům se tudíž nebrání ve výkonu jejich pravomocí, včetně pravomoci zastavit nebo zakázat předávání osobních údajů, pokud je předávání prováděno v rozporu s právem EU nebo vnitrostátním právem v oblasti ochrany údajů, například pokud dovozce údajů nedodržuje standardní smluvní doložky.[693]

Existence standardních doložek o ochraně údajů v právním rámci EU správcům nebrání, aby formulovali jiné ad hoc, individuální smluvní doložky, pokud je schválil dozorový úřad.[694] Budou však muset zajistit tutéž úroveň ochrany, jakou poskytují standardní doložky o ochraně údajů. Při schvalování ad hoc doložek jsou dozorové úřady povinny uplatňovat mechanismus jednotnosti, aby byl zajištěn jednotný regulační přístup v celé EU.[695] To znamená, že příslušný dozorový úřad musí oznámit návrh svého rozhodnutí o doložkách sboru EDPB. EDPB pak vydá stanovisko v dané věci a dozorový úřad musí toto stanovisko co nejvíce zohlednit při dalším postupu ve věci tohoto rozhodnutí. Pokud nemá v úmyslu se stanoviskem sboru EDPB řídit, bude zahájen mechanismus řešení sporů v rámci EDPB a sbor přijme závazné rozhodnutí.[696]

690 Tamtéž, čl. 46 odst. 2 písm. b) a čl. 46 odst. 5.

691 Tamtéž, čl. 46 odst. 2 písm. c); Smlouva o fungování Evropské unie, článek 288.

692 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, body 96–98 a 102–105.

693 Aby Komise zohlednila postoj SDEU ve věci *Schrems*, změnila své rozhodnutí o standardních smluvních doložkách. Prováděcí rozhodnutí Komise (EU) 2016/2297 ze dne 16. prosince 2016, kterým se mění rozhodnutí 2001/497/ES a 2010/87/EU o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí a zpracovatelům usazeným v těchto zemích podle směrnice Evropského parlamentu a Rady 95/46/ES, Úř. věst. 2016 L344.

694 Obecné nařízení o ochraně osobních údajů, čl. 46 odst. 3 písm. a).

695 Tamtéž, článek 63 a čl. 64 odst. 1 písm. e).

696 Tamtéž, článek 64 a článek 65.

Toto jsou nejdůležitější prvky standardních smluvních doložek:

- doložka pro příjemce, který je třetí stranou, jež umožňuje subjektům údajů vykonávat smluvní práva, ačkoliv nejsou stranou smlouvy,

- příjemce údajů nebo dovozce souhlasí, že se podřídí vnitrostátnímu dozorovému úřadu správce vyvážejícího údaje a/nebo jeho soudům v případě sporu.

Nyní platí dvě nové sady standardních doložek, které jsou k dispozici pro předávání údajů mezi správci, z nichž si správce údajů může vybrat.[697] Pro předávání mezi správcem a zpracovatelem platí pouze jediná sada standardních smluvních doložek.[698] Tyto standardní smluvní doložky jsou však v současnosti předmětem soudního řízení.

Příklad: Poté, co SDEU prohlásil rozhodnutí o „bezpečném přístavu" za neplatné,[699] nemohlo již být předávání osobních údajů do USA založeno na rozhodnutí o odpovídající ochraně. Zatímco probíhala jednání s orgány EU a než bylo přijato nové rozhodnutí o odpovídající ochraně (které bylo nakonec přijato 12. července 2016),[700] mohlo předávání probíhat pouze na základě jiných právních základů, jako jsou standardní smluvní doložky nebo závazná podniková pravidla. Několik společností, včetně společnosti Facebook Ireland (proti které byla podána žaloba, která vedla ke zrušení rozhodnutí o „bezpečném přístavu"), přešlo na standardní smluvní doložky, aby mohly pokračovat ve svém předávání údajů mezi EU a USA.

697 Sada I je obsažena v příloze rozhodnutí Evropské komise (2001), rozhodnutí Komise 2001/497/ES ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/46/ES, Úř. věst. 2001 L 181; sada II je uvedena v příloze rozhodnutí Evropské komise (2004), rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí, Úř. věst. 2004 L 385.

698 Evropská komise (2010), rozhodnutí Komise 2010/87 ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES, Úř. věst. 2010 L 39. V době sepisování této příručky bylo použití standardních smluvních doložek jako základu pro předávání osobních údajů do USA předmětem soudního řízení u irského vrchního soudu – High Court.

699 Rozsudek SDEU (velkého senátu) ze dne 6. října 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*.

700 Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí, Úř. věst. L 207.

Pan Schrems podal u irského dozorového úřadu stížnost, ve které úřad žádal, aby zastavil předávání údajů do USA na základě standardních smluvních doložek. V zásadě tvrdil, že pokud budou jeho osobní údaje předávány z irské pobočky společnosti Facebook společnosti Facebook Inc. a na servery nacházející se v USA, není nijak zaručeno, že budou chráněny. Společnost Facebook Inc. se řídí americkými zákony, které jí ukládají povinnost zpřístupnit osobní údaje donucovacím orgánům USA, a pro Evropany není k dispozici žádná soudní ochrana, v rámci níž by mohly tento postup napadnout.[701] Z těchto důvodů SDEU dospěl k závěru, že rozhodnutí o „bezpečném přístavu" je neplatné, a zatímco rozsudek soudu se omezoval na přezkum tohoto rozhodnutí, stěžovatel se domníval, že problémy, na které bylo poukázáno, jsou stejně relevantní i v případě předání na základě smluvních doložek. V době sepsání této příručky věc stále přezkoumával irský vrchní soud. Stěžovatel má zjevně v úmyslu postoupit věc SDEU, kde je jeho záměrem napadnout platnost rozhodnutí Evropské komise o standardních smluvních doložkách. Jak je popsáno v kapitole 5, pouze SDEU má pravomoc prohlásit určitý nástroj EU za neplatný.

Předání na základě závazných podnikových pravidel

Právo EU rovněž umožňuje předávání osobních údajů na základě závazných podnikových pravidel pro mezinárodní předávání, které probíhá v rámci téže skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost.[702] Než je možné se odvolávat na závazná podniková pravidla jako na nástroj pro předávání osobních údajů, musí je příslušný dozorový úřad schválit v souladu se závaznými podnikovými pravidly za použití mechanismu jednotnosti.

Mají-li být závazná podniková pravidla schválena, musí být právně závazná, zahrnovat veškeré základní zásady ochrany údajů a platit pro každého člena skupiny – a každý člen je musí prosazovat. Musí subjektům údajů výslovně přiznávat vymahatelná práva, zahrnovat veškeré nezbytné zásady ochrany údajů a splňovat určité formální požadavky, jako je uvedení struktury podniku, popis předávání a toho, jak budou uplatňovány zásady ochrany údajů. To zahrnuje poskytnutí těchto informací subjektům údajů. Závazná podniková pravidla musí mimo jiné uvádět práva subjektů

701 Pro více informací viz revidovanou stížnost na společnost Facebook Ireland Ltd předloženou irskému komisaři pro ochranu údajů (Irish Data Protection Commissioner) panem Maximilianem Schremsem dne 1. prosince 2015.

702 Obecné nařízení o ochraně osobních údajů, článek 47.

údajů a ustanovení o odpovědnosti za porušení pravidel.[703] Při schvalování závazných podnikových pravidel bude použit mechanismus pro spolupráci dozorových úřadů (popsán v kapitole 5).

V rámci mechanismu jednotnosti přezkoumává vedoucí dozorový úřad navrhovaná závazná podniková pravidla, přijímá návrhy rozhodnutí a oznamuje je sboru EDPB. Sbor vydává stanovisko v dané věci a vedoucí dozorový úřad může formálně schválit závazná podniková pravidla a současně „co nejvíce zohlední" stanovisko sboru. Toto stanovisko není právně závazné, ale pokud má dozorový úřad v úmyslu se stanoviskem neřídit, pak je zahájen mechanismus řešení sporů a bude nutné požádat sbor, aby přijal právně závazné rozhodnutí dvoutřetinovou většinou svých členů.[704]

Podle **práva RE** ad hoc nebo standardizované záruky, které jsou součástí právně závazného dokumentu,[705] rovněž zahrnují závazná podniková pravidla.

7.3.3. Výjimky pro zvláštní situace

Právo EU stanoví, že předávání osobních údajů do třetí země může být odůvodněné, a to i v případě, že nebylo vydáno rozhodnutí o odpovídající ochraně a neexistují vhodné záruky, jako jsou standardní smluvní doložky nebo závazná podniková pravidla, za kterékoliv z následujících okolností:

- subjekt údajů udělí výslovný souhlas s předáním údajů,
- subjekt údajů vstoupí – nebo se chystá vstoupit – do smluvního vztahu, jenž vyžaduje předání údajů do zahraničí,
- za účelem uzavření smlouvy mezi správcem údajů a třetí stranou v zájmu subjektu údajů,
- z důležitých důvodů veřejného zájmu,
- pro určení, výkon nebo obhajobu právních nároků,
- pro ochranu životně důležitých zájmů subjektu údajů,

703 Pro podrobnější popis viz obecné nařízení o ochraně osobních údajů, článek 47.

704 Tamtéž, čl. 57 odst. 1 písm. s), čl. 58 odst. 1 písm. j), čl. 64 odst. 1 písm. f), čl. 65 odst. 1 a 2.

705 Modernizovaná úmluva č. 108, čl. 14 odst. 3 písm. b).

- k předání údajů z veřejných rejstříků (jedná se o případ převažujících zájmů široké veřejnosti, pokud jde o přístup k informacím uloženým ve veřejných rejstřících).[706]

Jestliže neplatí žádná z těchto podmínek a předání není možné založit na rozhodnutí o odpovídající ochraně nebo vhodných zárukách, může k předání dojít pouze tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, pokud nejsou převáženy právy subjektu údajů.[707] V těchto případech správci musejí posoudit okolnosti daného předání údajů a poskytnout vhodné záruky. Musí také informovat dozorový úřad a subjekty údajů dotčené předáním o tomto předání i o závažných legitimních zájmech, které předání odůvodňují.

Skutečnost, že výjimky jsou poslední možností zákonného předávání údajů[708] (je třeba je používat pouze v případě, že nebylo vydáno rozhodnutí o odpovídající ochraně, a pokud nejsou zavedeny jiné záruky), zdůrazňuje jejich výjimečnou povahu a je dále podtržena v bodech odůvodnění GDPR.[709] Výjimky jsou jako také přijímány jako možnost „předat údaje za určitých okolností" na základě souhlasu, a pokud „je předání příležitostné a nezbytné"[710] v souvislosti se smluvními či právními nároky.

Kromě toho podle pokynů vydaných pracovní skupinou zřízenou podle článku 29 musí být spoléhání se na výjimky pro zvláštní situace výjimečné, založené na okolnostech jednotlivých případů a nemůže být použito v masivním měřítku a pro opakovaná předání.[711] Evropský inspektor ochrany údajů rovněž zdůraznil výjimečný charakter použití výjimek jako právního základu pro předání podle nařízení (ES) č. 45/2001 a konstatoval, že toto řešení by mělo být použito „v omezených případech" a „pro příležitostná předání".[712]

706 Obecné nařízení o ochraně osobních údajů, článek 49.

707 Tamtéž.

708 Tamtéž, čl. 49 odst. 1.

709 Viz obecné nařízení o ochraně osobních údajů, čl. 49 odst. 1 písm. a), b) a e) a 113. bod odůvodnění.

710 Tamtéž, čl. 49 odst. 1.

711 Pracovní skupina zřízená podle článku 29 (2005), *Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995*, WP 114, Brusel, 25. listopadu 2005.

712 Evropský inspektor ochrany údajů, *Předání osobních údajů ze strany orgánů a institucí EU třetím zemím a mezinárodním organizacím [The transfer of personal data to third countries and international organisations by EU institutions and bodies]*, stanovisko, Brusel, 14. července 2014, s. 15.

Příklad: Společnost Global Distribution System (GDS), která sídlí v USA, nabízí on-line rezervační systém pro více leteckých dopravců, hotelů a společností zajišťující výletní plavby po celém světě a zpracovává údaje desítek milionů osob v EU. Pro počáteční předání údajů na její servery v USA společnosti GDS uplatňovala výjimku jako právní základ pro předání. To bylo nezbytné pro uzavření smlouvy. Neuvádí tedy žádné jiné záruky pro osobní údaje pocházející z Evropy, které byly předány do USA a pak dále distribuovány hotelům po celém světě (to znamená, že nebyly poskytnuty žádné záruky ani pro následná předání). Společnost GDS neplní požadavky GDPR pro zákonné mezinárodní předávání údajů, protože se odvolává na výjimky jako zákonný důvod pro předávání v masivním měřítku.

Neplatí-li rozhodnutí o odpovídající ochraně, jsou EU nebo její členské státy oprávněny stanovit omezení pro předávání zvláštních kategorií osobních údajů do třetí země, navzdory tomu, že jsou splněny jiné podmínky pro tato předání, z důležitých důvodů veřejného zájmu. Tato omezení je třeba považovat za výjimečná a členské státy jsou povinny oznámit příslušná ustanovení Komisi.[713]

Právo RE umožňuje pohyby údajů na území, která nemají odpovídající ochranu údajů, v případě, že:

- subjekt údajů udělil souhlas,
- zájmy subjektu údajů toto předání vyžadují,
- existují převažující oprávněné zájmy, zejména důležité veřejné zájmy, stanovené zákonem,
- představuje nezbytné a přiměřené opatření v demokratické společnosti.[714]

7.3.4. Předání na základě mezinárodních dohod

EU může uzavřít mezinárodní dohody se třetími zeměmi, které upravují předávání osobních údajů za konkrétními účely. Tyto argumenty musejí zahrnovat vhodné

713 Viz obecné nařízení o ochraně osobních údajů, čl. 49 odst. 5.

714 Modernizovaná úmluva č. 108, čl. 14 odst. 4.

záruky k zajištění ochrany osobních údajů dotčených jednotlivců. GDPR platí, aniž by byly tyto mezinárodní dohody dotčeny.[715]

Členské státy mohou rovněž uzavřít mezinárodní dohody se třetími zeměmi nebo mezinárodními organizacemi, které zajišťují odpovídající úroveň ochrany základních práv a svobod jednotlivců, pokud tyto dohody nemají dopad na uplatňování GDPR.

Podobné pravidlo je stanoveno i v čl. 12 odst. 3 písm. a) Modernizované úmluvy č. 108.

K příkladům mezinárodních dohod zahrnujících předání osobních údajů patří dohody o jmenné evidenci cestujících.

Jmenná evidence cestujících

Údaje ve jmenné evidenci cestujících shromažďují letečtí dopravci při procesu rezervace letu a zahrnují mimo jiné jména, adresy, údaje o kreditních kartách a čísla sedadel cestujících v letecké dopravě. Letečtí dopravci rovněž shromažďují tyto informace pro své vlastní obchodní účely. EU uzavřela dohody s některými třetími zeměmi (Austrálie, Kanada a USA) pro předávání údajů jmenné evidence cestujících za účelem prevence, vyšetřování, odhalování či stíhání teroristických trestných činů nebo závažné nadnárodní trestné činnosti. Kromě toho Unie přijala v roce 2016 směrnici (EU) 2016/861 – označovanou také jako směrnici EU o jmenné evidenci cestujících[716]. Tato směrnice tvoří právní rámec pro členské státy EU, pokud jde o předávání údajů jmenné evidence cestujících příslušným orgánům v jiných třetích zemích, a to obdobně za účelem prevence, vyšetřování, odhalování či stíhání teroristických trestných činů nebo závažné trestné činnosti. Předávání údajů jmenné evidence cestujících orgánům třetích zemí se provádí jednotlivě a podléhá individuálnímu posouzení, zda je předání nezbytné pro účely uvedené ve směrnici, a za předpokladu, že jsou dodržována základní práva.

Pokud jde o dohody o jmenné evidenci cestujících mezi EU a třetími zeměmi, byla napadena jejich slučitelnost se základními právy na soukromí a ochranu údajů zakotvenými v Listině základních práv EU. Poté, co po uzavření jednání s Kanadou EU v roce 2014 podepsala dohodu o předávání a zpracování údajů jmenné evidence

715 Obecné nařízení o ochraně osobních údajů, 102. bod odůvodnění.

716 Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti, Úř. věst. 2016 L 119.

cestujících, rozhodl Evropský parlament, že postoupí věc SDEU, aby posoudil legalitu dohody s ohledem na právo EU a zejména s ohledem na články 7 a 8 Listiny.

Příklad: Ve svém posudku legality dohody mezi EU a Kanadou o jmenné evidenci cestujících[717] SDEU rozhodl, že ve své stávající podobě není zamýšlená dohoda slučitelná se základními právy uznávanými Listinou, a proto není možné ji uzavřít. Jelikož zahrnovala zpracování osobních údajů, jednalo se o zásah do práva na ochranu osobních údajů, které je chráněno podle článku 8 Listiny. Současně také představuje omezení práva na respektování soukromého života, které je zakotveno v článku 7, jelikož jako celek mohou být údaje jmenné evidence cestujících agregovány a analyzovány způsobem, který odhaluje cestovní návyky, vztahy mezi různými jednotlivci, informace o jejich finanční situaci, o jejich stravovacích návycích a zdravotním stavu, a tudíž mají dopad na jejich soukromý život.

Zásah do základních práv, který přinesla zamýšlená dohoda, sledoval cíl obecného zájmu, konkrétně veřejné bezpečnosti a boje proti terorismu a závažné přeshraniční trestné činnosti. SDEU však připomněl, že má-li být zásah odůvodněný, musí se omezit na to, co je nezbytně nutné k dosažení sledovaného cíle. Po provedení analýzy ustanovení dohody dospěl SDEU k závěru, že zamýšlená dohoda nesplňuje kritérium „naprosté nutnosti". Mezi faktory, které SDEU zvážil, než dospěl k rozhodnutí patří toto:

- Skutečnost, že zamýšlená dohoda zahrnuje předávání citlivých údajů. Údaje jmenné evidence cestujících nashromážděné podle zamýšlené dohody by mohly zahrnovat citlivé údaje, jako jsou informace odhalující rasový či etnický původ, náboženské přesvědčení či zdravotní stav cestujících. Předávání a zpracování citlivých údajů kanadskými orgány by mohlo představovat riziko pro zásadu zákazu diskriminace, a tudíž vyžaduje přesné a pádné odůvodnění na jiném základě, než je ochrana veřejné bezpečnosti a boj proti závažné trestné činnosti. Zamýšlená dohoda toto odůvodnění neposkytuje.[718]

- Další ukládání údajů jmenné evidence cestujících u všech cestujících po dobu pěti let, dokonce i když cestující cestovali z Kanady, bylo považováno za opatření, které překračuje meze toho, co je naprosto nutné. SDEU

717 SDEU, *Posudek 1/15 Soudního dvora (velkého senátu)*, 26. července 2017.

718 Tamtéž, bod 165.

> se domníval, že by bylo přípustné, aby kanadské orgány uchovávaly údaje o cestujících, kteří podle objektivních důkazů mohou představovat ohrožení veřejné bezpečnosti, i poté, co tyto osoby opustí kanadské území. Naproti tomu ukládání osobních údajů *všech* cestujících, u kterých neexistují ani nepřímé důkazy, že představují riziko pro veřejnou bezpečnost, není odůvodněné.[719]

Poradní výbor podle úmluvy č. 108 vydal stanovisko k důsledkům dohod o jmenné evidenci cestujících pro ochranu údajů podle práva RE.[720]

Předávání údajů o transakcích

Společnost pro celosvětovou mezibankovní finanční telekomunikaci (SWIFT) se sídlem v Belgii, která je zpracovatelem většiny celosvětových peněžních převodů z evropských bank, provozovala „zrcadlové" středisko v USA a byla postavena před žádost o zveřejnění údajů ze strany Ministerstva financí USA za účelem vyšetřování terorismu v rámci jeho Programu sledování financování terorismu.[721]

Z hlediska EU neexistoval dostatečný právní základ pro zpřístupnění těchto údajů – především o občanech v EU – Spojeným státům jednoduše z toho důvodu, že se zde nacházelo pouze jedno ze středisek zpracovávání služby v oblasti údajů společnosti SWIFT.

719 Tamtéž, body 204–207.

720 Rada Evropy, *Opinion on the Data protection implications of the processing of Passenger Name Records* [Stanovisko k důsledkům zpracovávání jmenné evidence cestujících pro ochranu údajů], T-PD(2016)18rev, 19. srpna 2016.

721 Viz v této souvislosti pracovní skupina zřízená podle článku 29 (2011), *Stanovisko 14/2011 k otázkám ochrany údajů v souvislosti s předcházením praní peněz a financování terorismu*, WP 186, Brusel, 13. června 2011; pracovní skupina zřízená podle článku 29 (2006), *Stanovisko 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication (SWIFT))*, WP 128, Brusel, 22. listopadu 2006; Belgická komise pro ochranu soukromí (*Commission de la protection de la vie privée*) (2008), *„Control and recommendation procedure initiated with respect to the company SWIFT scrl"* [Řízení o zahájení kontroly a vydání doporučení zahájené proti společnosti SWIFT scrl], rozhodnutí, 9. prosince 2008.

V roce 2010 byla uzavřena zvláštní dohoda mezi EU a USA, známá též jako dohoda o SWIFT, která stanovila nezbytný právní základ a zajistila odpovídající normy ochrany údajů.[722]

Podle této dohody jsou finanční údaje ukládané společností SWIFT i nadále poskytovány Ministerstvu financí USA za účelem prevence, vyšetřování, odhalování či stíhání terorismu nebo financování terorismu. Ministerstvo financí USA může požádat o finanční údaje od společnosti SWIFT, pokud žádost:

- co nejzřetelněji označí finanční údaje,
- jasně zdůvodní nezbytnost dotyčných údajů,
- je formulována co nejkonkrétněji, aby bylo co nejvíce minimalizováno množství požadovaných údajů,
- nemá za cíl získat údaje týkající se jednotné oblasti pro platby v eurech (SEPA).[723]

Europol musí obdržet kopii každé žádosti předložené Ministerstvem financí USA a ověřit, zda jsou dodrženy zásady dohody o SWIFT.[724] Pokud se potvrdí, že jsou v souladu, musí společnost SWIFT poskytnout finanční údaje přímo Ministerstvu financí USA. Ministerstvo musí finanční údaje ukládat ve fyzicky zabezpečeném prostředí, kde k nim mohou mít přístup pouze analytici, kteří se zabývají vyšetřováním terorismu nebo jeho financováním, a tyto finanční údaje nesmí být propojeny s jakoukoli jinou databází. Obecně pak musejí být finanční údaje přijaté společností SWIFT smazány nejpozději do pěti let od přijetí. Finanční údaje, které jsou relevantní pro konkrétní vyšetřování nebo stíhání, mohou být uchovávány tak dlouho, dokud jsou pro toto vyšetřování nebo stíhání nezbytné.

Ministerstvo financí USA může předat informace z údajů obdržených od společnosti SWIFT konkrétním donucovacím orgánům, orgánům veřejné bezpečnosti nebo orgánům pověřeným bojem proti terorismu na území USA i mimo ně výlučně pro účely vyšetřování, odhalování či stíhání terorismu nebo financování terorismu. Pokud se

722 Rozhodnutí Rady 2010/412/EU ze dne 13. července 2010 o uzavření Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu sledování financování terorismu, Úř. věst. 2010 L 195, s. 3 a 4. Znění dohody je přílohou tohoto rozhodnutí, Úř. věst. 2010 L 195, s. 5–14.

723 Tamtéž, čl. 4 odst. 2.

724 Společný kontrolní orgán Europolu provedl audity činností Europolu v této oblasti.

toto další předání finančních údajů týká občana nebo rezidenta členského státu EU, je jakékoliv sdílení údajů s orgány třetí země podmíněno předchozím souhlasem příslušných orgánů dotyčného členského státu. Je možné stanovit výjimky, pokud má sdílení údajů zásadní význam pro zabránění bezprostřednímu a závažnému ohrožení veřejné bezpečnosti.

Dodržování zásad uvedených v dohodě o SWIFT monitorují nezávislé subjekty, včetně osoby jmenované Evropskou komisí. Mají možnost přezkoumávat v reálném čase i zpětně všechna vyhledávání v poskytovaných údajích, pravomoc žádat o další informace za účelem vysvětlení spojitosti s terorismem u těchto vyhledávání a pravomoc některá nebo všechna vyhledávání blokovat, ukáže-li se, že byla provedena v rozporu se zárukami stanovenými v dohodě.

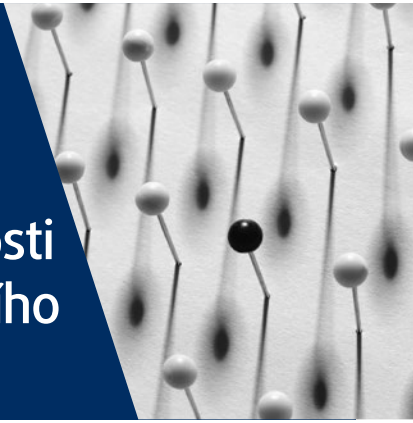
Subjekty údajů mají právo získat potvrzení od příslušného orgánu dohledu EU, že byla dodržena jejich práva na ochranu osobních údajů. Subjekty údajů také mají právo na opravu, výmaz nebo blokování jejich údajů, které byly shromážděny a uloženy Ministerstvem financí USA podle dohody o SWIFT. Práva subjektů údajů na přístup však mohou podléhat určitým právním omezením. Je-li přístup zamítnut, musí být subjekty údajů písemně o tomto zamítnutí informovány a rovněž musí být informovány o svém právu požadovat správní a soudní nápravu v USA.

Dohoda o SWIFT platí po dobu pěti let a její první období platnosti trvalo do srpna 2015. Automaticky se prodlužuje na další období v délce jednoho roku, pokud jedna ze stran neuvědomí druhou stranu s alespoň šestiměsíčním předstihem o svém záměru dohodu neprodloužit. Automatické prodlužování se použilo v srpnu 2015, 2016 a 2017 a zajišťuje platnost dohody o SWIFT přinejmenším do srpna 2018.[725]

725 Tamtéž, čl. 23 odst. 2.

8

Ochrana údajů v souvislosti s činností policie a trestního soudnictví



EU	Pojednávaná témata	RE
Směrnice o ochraně údajů policií a trestním soudnictvím	**Obecně**	Modernizovaná úmluva č. 108
	Policie	Doporučení o policii Praktická příručka o používání osobních údajů v policejním sektoru
	Dohled	Rozsudek ESLP z roku 2009, *B.B. v. Francie*, č. 5335/06 Rozsudek ESLP (velkého senátu) z roku 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04 Rozsudek ESLP z roku 2002, *Allan v. Spojené království*, č. 48539/99 Rozsudek ESLP z roku 1984, *Malone v. Spojené království*, č. 8691/79 Rozsudek ESLP z roku 1978, *Klass a další v. Německo*, č. 5029/71 Rozsudek ESLP z roku 2016, *Szabó a Vissy v. Maďarsko*, č. 37138/14 Rozsudek ESLP z roku 2005, *Vetter v. Francie*, č. 59842/00
	Kyberkriminalita	Úmluva o počítačové kriminalitě

EU	Pojednávaná témata	RE
Jiné zvláštní právní nástroje		
Prümské rozhodnutí	**Pro zvláštní údaje: otisky prstů, DNA, výtržnictví, informace o cestujících v letecké dopravě, údaje o telekomunikacích atd.**	Modernizovaná úmluva č. 108, článek 6 Doporučení o policii, Praktická příručka o používání osobních údajů v policejním sektoru
Švédská iniciativa (rámcové rozhodnutí Rady 2006/960/SVV)	**Zjednodušení výměny informací, včetně zpravodajských, mezi donucovacími orgány**	Rozsudek ESLP (velkého senátu) z roku 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04
Směrnice (EU) 2016/681 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti Rozsudek SDEU (velkého senátu) z roku 2014, spojené věci C-293/12 a C-594/12, Digital Rights Ireland a Kärntner Landesregierung a další Rozsudek SDEU (velkého senátu) z roku 2016, spojené věci C-203/12 a C-698/15, Tele2 Sverige a Home Department v. Tom Watson a další	**Uchovávání osobních údajů**	Rozsudek ESLP z roku 2009, *B.B. v. Francie*, č. 5335/06
Nařízení o Europolu Rozhodnutí o Eurojustu	**Zvláštními agenturami**	Doporučení o policii
Rozhodnutí Schengen II Nařízení o systému VIS Nařízení o systému Eurodac Rozhodnutí o systému CIS	**Zvláštními společnými informačními systémy**	Doporučení o policii Rozsudek ESLP z roku 2010, *Dalea v. Francie*, č. 964/07

RE i EU vytvořily zvláštní právní nástroje s cílem vyvážit zájmy jednotlivců na ochraně údajů a zájmy společnosti na shromažďování údajů pro účely boje proti trestné činnosti a zajištění národní a veřejné bezpečnosti. Tento oddíl nabízí přehled práva RE (oddíl 8.1) a práva EU (oddíl 8.2) v souvislosti s ochranou údajů ve věcech týkajících se policie a trestního soudnictví.

8.1. Právo RE v souvislosti s věcmi týkajícími se ochrany údajů a národní bezpečnosti, policie a trestního soudnictví

Hlavní body

- Modernizovaná úmluva č. 108 a doporučení o policii RE se vztahují na ochranu údajů ve všech oblastech policejní činnosti.
- Úmluva o počítačové kriminalitě (Budapešťská úmluva) je závazný mezinárodní právní nástroj zabývající se trestnými činy spáchanými proti elektronickým sítím nebo jejich prostřednictvím. Je rovněž relevantní pro vyšetřování nekybernetických trestných činů, jejichž součástí jsou elektronické důkazy.

Jedním významným rozdílem mezi právem RE a EU je to, že **právo RE** se na rozdíl od práva EU vztahuje i na oblast národní bezpečnosti. To znamená, že smluvní strany musejí dodržovat článek 8 EÚLP i v případě činností, které souvisejí s národní bezpečností. Činností státu v citlivých oblastech práva a praxe národní bezpečnosti se týká několik rozsudků ESLP.[726]

Pokud jde o policii a trestní soudnictví na evropské úrovni, zahrnuje Modernizovaná úmluva č. 108 všechny oblasti zpracování osobních údajů a její ustanovení mají upravovat zpracování osobních údajů obecně. Modernizovaná úmluva č. 108 se tedy použije na i zpracování údajů v policejní oblasti a v oblasti trestního soudnictví. Zpracování genetických údajů, osobních údajů souvisejících s trestnými činy, trestním řízením a odsouzením za trestné činy a souvisejících bezpečnostních opatření, biometrických údajů umožňujících jedinečnou identifikaci fyzické osoby, jakož i jakýchkoliv citlivých osobních údajů, je povoleno pouze tehdy, pokud existují záruky před riziky, které může zpracování těchto údajů představovat pro zájmy, práva a základní svobody subjektu údajů, zejména riziko diskriminace.[727]

Právní úkoly policejních orgánů a orgánů trestního soudnictví často vyžadují zpracovávání osobních údajů, které mohou mít vážné důsledky pro dotčené jednotlivce. Doporučení o policii přijaté RE v roce 1987 udílí pokyny členským státům RE o tom,

726 Viz například rozsudek ESLP ze dne 6. září 1978, *Klass a další v. Německo*, č. 5029/71; rozsudek ESLP (velkého senátu) ze dne 4. května 2000, *Rotaru v. Rumunsko*, č. 28341/95 a rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy v. Maďarsko*, č. 37138/14.

727 Modernizovaná úmluva č. 108, článek 6.

jak by měly naplňovat zásady uvedené v úmluvě č. 108 v souvislosti se zpracováním osobních údajů policejními orgány.[728] Doporučení bylo doplněno praktickou příručkou o používání osobních údajů v policejním sektoru, kterou přijal Poradní výbor podle úmluvy č. 108.[729]

Příklad: Ve věci *D.L. v. Bulharsko*[730] umístily sociální služby stěžovatele do zabezpečené vzdělávací instituce na základě soudního příkazu. Veškerá písemná korespondence a telefonické rozhovory podléhaly plošnému a všeobecnému dohledu ze strany této instituce. ESLP konstatoval, že došlo k porušení článku 8, jelikož dané opatření nebylo v demokratické společnosti nezbytné. Soud konstatoval, že bylo nutné vynaložit maximální úsilí, aby umožnil nezletilým osobám umístěným v instituci mít dostatečný kontakt s vnějším světem, protože se jedná o nedílnou součást jejich práva na to, aby s nimi bylo zacházeno důstojně, a bylo absolutně nezbytné připravit se na jejich opětovné začlenění do společnosti. To se týká jak návštěv, tak písemné korespondence nebo telefonických hovorů. Kromě toho dohled nijak nerozlišoval mezi komunikací s rodinnými příslušníky a nevládními organizacemi zastupujícími práva dětí nebo s právními zástupci. Kromě toho, rozhodnutí odposlouchávat komunikaci nebylo založeno na individualizované analýze rizik v každém konkrétním případě.

Příklad: Ve věci *Dragojević v. Chorvatsko*[731] byl stěžovatel podezřelý z toho, že se podílel na pašování drog. Byl shledán vinným poté, co vyšetřující soudce povolil použití opatření tajného sledování s cílem odposlouchávat telefonní hovory stěžovatele. ESLP rozhodl, že opatření, proti kterému se podává stížnost, představuje zásah do práva na respektování soukromého života a korespondence. Povolení vydané vyšetřujícím soudcem bylo založeno pouze na tvrzení stíhajícího orgánu, že „vyšetřování nemohlo být provedeno jinými prostředky". ESLP rovněž konstatoval, že trestní soudy omezily své posuzování, pokud jde o použití opatření v oblasti sledování, a že veřejná správa neuplatnila právní ochranu, která je k dispozici. Došlo tedy k porušení článku 8.

728 Rada Evropy, Výbor ministrů (1987), Doporučení Rec(87)15 Výboru ministrů členským státům upravující používání osobních údajů v policejním sektoru, 17. září 1987.

729 Rada Evropy (2018), Poradní výbor podle úmluvy č. 108, Practical Guide on the use of personal data in the police sector [Praktická příručka o používání osobních údajů v policejním sektoru], T-PD(2018)1.

730 Rozsudek ESLP ze dne 19. května 2016, *D.L. v. Bulharsko*, č. 7472/14.

731 Rozsudek ESLP ze dne 15. ledna 2015, *Dragojević v. Chorvatsko*, č. 68955/11.

8.1.1. Doporučení o policii

ESLP soudržně rozhodl, že ukládání a uchovávání osobních údajů policejními orgány a orgány národní bezpečnosti představuje zásah do čl. 8 odst. 1 EÚLP. Řada rozsudků ESLP se zabývá odůvodněním takového zásahu.[732]

Příklad: Ve věci *B.B. v. Francie*[733] byl stěžovatel odsouzen za účast na sexuálních trestných činech proti 15letým nezletilým jako osoba požívající jejich důvěry. V roce 2000 dokončil výkon svého trestu odnětí svobody. O rok později požádal, aby byl záznam o tomto rozsudku odstraněn z jeho trestního rejstříku, ale žádost byla zamítnuta. V roce 2004 jeden francouzský zákon zřídil vnitrostátní soudní databázi pachatelů sexuálních trestných činů a stěžovatel byl informován o tom, že je na tento seznam zapsán. ESLP konstatoval, že zapsání odsouzeného pachatele trestného činu do vnitrostátní soudní databáze spadá do působnosti článku 8 EÚLP. Avšak vzhledem k tomu, že byly zavedeny odpovídající záruky ochrany údajů, jako je právo subjektu údajů požádat o výmaz údajů, omezená délka ukládání údajů a omezený přístup k těmto údajům, bylo dosaženo spravedlivé rovnováhy mezi dotčenými soukromými a veřejnými zájmy, které se zde střetávají. Soud shledal, že nedošlo k porušení článku 8 EÚLP.

Příklad: Ve věci *S. a Marper v. Spojené království*[734] byli oba stěžovatelé obviněni ze spáchání trestných činů, avšak nebyli odsouzeni. Přesto policie uchovávala a ukládala jejich otisky prstů, buněčné vzorky a profily DNA. Neomezené uchovávání výše uvedených biometrických údajů bylo povoleno právním předpisem, pokud je osoba podezřelá ze spáchání trestného činu, i když byl podezřelý později zproštěn obvinění nebo propuštěn. ESLP konstatoval, že plošné a všeobecné uchovávání osobních údajů, které nebylo časově omezené a u něhož měli jednotlivci zproštění obvinění jen omezené možnosti, jak požádat o výmaz, představovalo nepřiměřený zásah do práv žadatelů na respektování soukromého života. Soud rozhodl, že došlo k porušení článku 8 EÚLP.

732 Viz například rozsudek ESLP ze dne 26. března 1987, *Leander v. Švédsko*, č. 9248/81; rozsudek ESLP ze dne 13. listopadu 2012, *M.M. v. Spojené království*, č. 24029/07; rozsudek ESLP ze dne 18. dubna 2013, *M.K. v. Francie*, č. 19522/09 nebo rozsudek ESLP ze dne 22. června 2017, *Aycaguer v. Francie*, č. 8806/12.

733 Rozsudek ESLP ze dne 17. prosince 2009, *B.B. v. Francie*, č. 5335/06.

734 Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2008, *S. a Marper v. Spojené království*, č. 30562/04 a 30566/04, body 119 a 125.

Jedním ze zásadních problémů v souvislosti s elektronickými komunikacemi je zásah orgánů veřejné moci do práva na soukromí a na ochranu údajů. Prostředky sledování nebo odposlouchávání komunikací, jako jsou odposlouchávací nebo příposlechová zařízení, jsou přípustné pouze tehdy, pokud je to stanoveno zákonem a pokud to představuje nezbytné opatření v demokratické společnosti v zájmu:

- ochrany bezpečnosti státu,
- veřejné bezpečnosti,
- finančních zájmů státu,
- potírání trestných činů nebo
- ochrany subjektu údajů nebo práv a svobod jiných osob.

Řada dalších rozsudků ESLP se zabývá odůvodněním zásahu do práva na soukromí prostřednictvím provádění sledování.

Příklad: Ve věci *Allan v. Spojené království*[735] orgány tajně nahrávaly soukromé rozhovory mezi vězněm a jeho přítelem v oblasti věznice určené pro návštěvy a rovněž rozhovory se spoluobviněným ve vězeňské cele. ESLP konstatoval, že použití zařízení pro pořizování audio a videozáznamu ve stěžovatelově cele, oblasti věznice určené pro návštěvy a v případě spoluvězně představuje zásah do stěžovatelova práva na soukromý život. Protože neexistovala zákonná úprava, která by v relevantní době regulovala používání tajných nahrávacích zařízení ze strany policie, nebyl tento zásah v souladu se zákonem. Soud proto shledal, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Roman Zakharov v. Rusko*[736] stěžovatel zahájil soudní řízení proti třem operátorům mobilních sítí. Tvrdil, že jeho právo na soukromí, pokud jde o elektronické komunikace, bylo porušeno, protože operátoři nainstalovali zařízení umožňují Federální bezpečnostní službě odposlouchávat jeho telefonickou komunikaci bez předchozího soudního povolení. ESLP konstatoval, že vnitrostátní právní ustanovení upravující odposlouchávání komunikací nestanovila odpovídající a účinné záruky proti svévoli a riziku zneužívání.

735 Rozsudek ESLP ze dne 5. listopadu 2002, *Allan v. Spojené království*, č. 48539/99.

736 Rozsudek ESLP (velkého senátu) ze dne 4. prosince 2015, *Roman Zakharov v. Rusko*, č. 47143/06.

Zejména vnitrostátní právo neukládalo povinnost smazat uložené údaje poté, co byl naplněn účel ukládání. Kromě toho, ačkoliv bylo vyžadováno soudní povolení, byla soudní kontrola omezená.

Příklad: Ve věci *Szabó a Vissy v. Maďarsko*[737] stěžovatelé tvrdili, že maďarské právní předpisy jsou v rozporu s článkem 8 EÚLP, protože nejsou dostatečně podrobné a přesné. Kromě toho byl předložen argument, že právní předpisy nestanovují dostatečné záruky proti zneužívání a svévoli. ESLP rozhodl, že maďarské právo neukládá povinnost, aby dohled podléhal povolení soudem. Soud přesto konstatoval, že i když tento dohled podléhal schválení ministrem spravedlnosti, byl zjevně politické povahy a nebylo možné zaručit požadované posouzení „naprosté nezbytnosti". Kromě toho nestanovilo vnitrostátní právo soudní přezkum, jelikož subjektům nebylo zasláno žádné oznámení. Soud rozhodl, že došlo k porušení článku 8 EÚLP.

Jelikož zpracování údajů policejními orgány může mít zásadní dopad na dotčené osoby, jsou v této oblasti zvlášť nezbytná podrobná pravidla ochrany údajů pro zpracování osobních údajů. Doporučení o policii RE se snažilo tento problém ošetřit tím, že poskytlo pokyny, jak by měly být shromažďovány osobní údaje pro účely policejní práce; jak by měly být uchovávány soubory údajů v této oblasti; kdo by měl mít povolen přístup k těmto souborům, včetně podmínek pro předávání osobních údajů zahraničním policejním orgánům; jak by měly být subjekty údajů schopny vykonávat svá práva v souvislosti s ochranou údajů a jak by měla být prováděna kontrola ze strany nezávislých orgánů. Rovněž byla pojednána povinnost zajistit dostatečnou bezpečnost údajů.

Doporučení nestanovilo neomezené shromažďování osobních údajů policejními orgány bez omezení délky. Omezuje shromažďování osobních údajů policejními orgány na to, co je nezbytné za účelem zabránění skutečnému nebezpečí nebo vyšetřování konkrétního trestného činu. Jakékoliv další shromažďování údajů bude muset být založeno na konkrétních vnitrostátních právních předpisech. Zpracování citlivých údajů by se mělo omezovat na to, co je naprosto nezbytné v souvislosti s daným vyšetřováním.

Pokud se osobní údaje shromažďují bez vědomí subjektu údajů, musí být subjekt údajů informován o shromažďování údajů, jakmile již toto zveřejnění není překážkou

737 Rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy v. Maďarsko*, č. 37138/14.

pro vyšetřování. Shromažďování údajů formou sledování technickými prostředky nebo jinými automatizovanými prostředky musí mít konkrétní právní základ.

Příklad: Ve věci *Versini-Campinchi a Crasnianski v. Francie*[738] stěžovatelka, která je advokátka, měla telefonický rozhovor s klientem, jehož telefonní linka byla na žádost vyšetřujícího soudce odposlouchávána. Přepis hovoru svědčil o tom, že zveřejnila informace, na které se vztahuje povinnost advokátní mlčenlivosti. Státní zástupce zaslal tuto informaci advokátní komoře, která udělila stěžovatelce pokutu. ESLP uznal, že došlo k zásahu do práva na respektování soukromého života a korespondence, a to nejen osoby, jejíž telefon byl odposlouchávána, ale také stěžovatelky, jejíž komunikace byla odposlouchávána a přepisována. Zásah byl proveden v souladu se zákonem a sledoval legitimní cíl, jímž bylo zabránit narušení veřejného pořádku. Stěžovatelka dosáhla přezkumu zákonnosti předložení přepisu nahrávky pořízené pomocí odposlouchávání telefonu v souvislosti s disciplinárním řízením, které proti ní bylo vedeno. Ačkoliv neuspěla se žádostí o prohlášení přepisu telefonického rozhovoru za neplatný, ESLP se domníval, že došlo k účinnému přezkumu, který je schopen omezit zásah, na který si stěžovatelka stěžovala, na to, co je nezbytné v demokratické společnosti. ESLP konstatoval, že argument, že možnost trestního řízení proti advokátce na základě přepisu mohla mít odrazující dopad na svobodu komunikace mezi advokátkou a jejím klientem, a tudíž na práva klienta na obhajobu, nebyl věrohodný, pokud skutečnosti zveřejněné samotnou advokátkou mohly představovat nezákonné jednání této osoby. Bylo tedy konstatováno, že nedošlo k porušení článku 8.

Doporučení o policii RE stanoví, že při ukládání osobních údajů je třeba jasně rozlišovat mezi: správními údaji a policejními údaji; osobními údaji jednotlivých typů subjektů údajů, jako jsou podezřelí, obvinění, oběti a svědkové; a údaji považovanými za nezpochybnitelné skutečnosti a těmi, které jsou založeny na podezření nebo spekulaci.

Účel, pro který může policie údaje používat, musí být důsledně omezen. To má důsledky pro zpřístupnění policejních údajů třetím stranám: předání nebo zpřístupnění těchto údajů v rámci policejního sektoru by se mělo řídit tím, zda existuje legitimní zájem na sdílení dané informace, či nikoliv. Předání nebo zpřístupnění těchto údajů mimo policejní sektor by mělo být povoleno pouze tehdy, pokud existuje jasná právní povinnost nebo povolení.

738 Rozsudek ESLP ze dne 16. června 2016, *Versini-Campinchi a Crasnianski v. Francie*, č. 49176/11.

Příklad: Ve věci *Karabeyoğlu v. Turecko*[739] byly sledovány telefonické linky stěžovatele, který je profesí soudce, v souvislosti s trestním vyšetřováním nelegální organizace, ke které měl podle podezření patřit nebo o níž se mělo za to, že jí stěžovatel poskytuje pomoc a podporu. V návaznosti na rozhodnutí nezahájit stíhání státní zástupce pověřený vedením trestněprávního vyšetřování dotčené nahrávky zničil. Avšak jejich kopie zůstala v držení soudních vyšetřovatelů, kteří dotčený materiál následně použili v souvislosti s disciplinárním vyšetřováním stěžovatele. ESLP rozhodl, že byly porušeny příslušné právní předpisy, protože informace byly použity pro jiné účely, než byly ty, pro které byly shromážděny, a nebyly zničeny ve lhůtě stanovené právními předpisy. Zásah do práva stěžovatele na respektování jeho soukromého života nebyl v souladu se zákonem, pokud jde o disciplinární řízení, které proti němu bylo vedeno.

Mezinárodní předání nebo zpřístupnění by mělo být omezeno na zahraniční policejní orgány a mělo by být založeno na zvláštních právních ustanoveních, pokud možno mezinárodních dohodách, ledaže je to nezbytné pro předcházení závažnému a bezprostřednímu nebezpečí.

Zpracování údajů ze strany policie musí podléhat nezávislému dozoru s cílem zajistit soulad s vnitrostátním právem v oblasti ochrany údajů. Subjekty údajů musí mít veškerá práva na přístup obsažená v Modernizované úmluvě č. 108. Pokud byla práva subjektů údajů na přístup omezena podle článku 9 úmluvy č. 108 v zájmu účinných policejních vyšetřování a výkonu trestů, musí mít subjekt údajů podle vnitrostátního práva právo na odvolání se k vnitrostátnímu dozorovému úřadu pro ochranu údajů nebo k jinému nezávislému orgánu.

8.1.2. Budapešťská úmluva o počítačové kriminalitě

Jelikož se při trestné činnosti stále více používají elektronické systémy zpracování údajů, a protože má tato činnost na tyto systémy stále větší dopad, jsou zapotřebí nová trestněprávní ustanovení, která se budou touto výzvou zabývat. RE proto přijala mezinárodní právní nástroj – úmluvu o počítačové kriminalitě, rovněž označovanou jako budapešťskou úmluvu –, která se má zabývat trestnou činností spáchanou proti elektronickým sítím a jejich prostřednictvím.[740] K této úmluvě mohou přistoupit také nečlenské země RE. Na začátku roku 2018 bylo stranou úmluvy 14 států, které

739 Rozsudek ESLP ze dne 7. června 2016, *Karabeyoğlu v. Turecko*, č. 30083/10.

740 Rada Evropy, Výbor ministrů (2001), Úmluva o počítačové kriminalitě, CETS č. 185, Budapešť, 23. listopadu 2001, vstoupila v platnost dne 1. července 2004.

nejsou členy RE[741], a sedm další nečlenských zemí bylo přizváno, aby se k úmluvě připojilo.

Úmluva o počítačové kriminalitě je i nadále nejvlivnější mezinárodní smlouvou, která se zabývá porušením práva prostřednictvím internetu nebo jiných informačních sítí. Ukládá stranám povinnost aktualizovat a harmonizovat trestněprávní předpisy týkající se hackingu a jiných forem narušení zabezpečení, včetně porušení autorského práva, podvodů prostřednictvím počítače, dětské pornografie a jiných protiprávních kybernetických činností. Úmluva také stanoví procesní pravomoci, které zahrnují vyhledávání počítačových sítí a odposlouchávání komunikací v souvislosti s bojem proti kybernetické trestné činnosti. V neposlední řadě umožňuje účinnou mezinárodní spolupráci. Dodatkový protokol k úmluvě se zabývá kriminalizací rasistické a xenofobní propagandy v počítačových sítích.

Ačkoliv úmluva není nástrojem, který by měl za cíl propagaci ochrany údajů, kriminalizuje činnosti, které jsou pravděpodobně v rozporu s právem subjektu údajů na ochranu jeho osobních údajů. Kromě toho ukládá smluvním stranám povinnost přijmout legislativní opatření, které jejich vnitrostátním orgánům umožní odposlouchávání provozních a obsahových dat.[742] Rovněž zavazuje smluvní strany, aby při provádění úmluvy stanovily přiměřenou ochranu lidských práv a svobod, včetně práv zaručených EÚLP, jako je právo na ochranu údajů.[743] Smluvní strany nejsou povinny se také připojit k Úmluvě č. 108, aby se mohly připojit k budapešťské úmluvě o počítačové kriminalitě.

741 Austrálie, Dominikánská republika, Chile, Izrael, Japonsko, Kanada, Kolumbie, Mauricius, Panama, Senegal, Spojené státy, Srí Lanka, Tonga a Tunisko. Viz Tabulku s podpisy a ratifikacemi Smlouvy 185, stav k červenci 2017.

742 Rada Evropy, Výbor ministrů (2001), Úmluva o počítačové kriminalitě, CETS č. 185, Budapešť, 23. listopadu 2001, článek 20 a 21.

743 Tamtéž, čl. 15 odst. 1.

8.2. Právo EU v oblasti ochrany údajů ve věcech týkajících se policie a trestního soudnictví

Hlavní body

- V rámci EU je ochrana údajů v odvětví policie a trestního soudnictví upravena, pokud jde jak o vnitrostátní, tak o přeshraniční zpracovávání policejními orgány a orgány trestního soudnictví členských států a subjektů EU.
- Na úrovni členských států je třeba začlenit do vnitrostátního práva směrnici o ochraně údajů policií a trestním soudnictvím.
- Ochranu údajů v oblasti přeshraniční spolupráce policie a donucovacích orgánů, zejména v boji proti terorismu a přeshraniční trestné činnosti, upravují zvláštní právní nástroje.
- Zvláštní pravidla pro ochranu údajů existují pro Evropský policejní úřad (Europol), jednotku EU pro soudní spolupráci (Eurojust) a nově zřízený Úřad evropského veřejného žalobce, což jsou orgány EU, které pomáhají přeshraničnímu prosazování práva a podporují je.
- Zvláštní pravidla na ochranu údajů existují i pro společné informační systémy, které byly zřízeny na úrovni EU za účelem přeshraniční výměny informací mezi příslušnými policejními a soudními orgány. K významným příkladům patří Schengenský informační systém II (SIS II), Vízový informační systém (VIS) a systém Eurodac, což je centralizovaný systém obsahující údaje o otiscích prstů státních příslušníků třetí země a osob bez státního občanství, kteří žádají o azyl v jednom ze členských států EU.
- EU v současnosti aktualizuje výše uvedená ustanovení týkající se ochrany údajů, aby byla v souladu s ustanovením směrnice o ochraně údajů policií a trestním soudnictvím.

8.2.1. Směrnice o ochraně údajů policií a trestním soudnictvím

Směrnice 2016/680/EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů (směrnice

o ochraně údajů policií a trestním soudnictvím)[744] má za cíl chránit osobní údaje shromážděné a zpracovávané pro účely trestního soudnictví, ke kterým patří:

- prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení,
- výkon trestu a
- v případech, kdy policie a jiné donucovací orgány jednají za účelem dodržování práva a za účelem ochrany před hrozbami pro veřejnou bezpečnost a pro základní práva společnosti, které by mohly být kvalifikovány jako trestný čin, a k předcházení těmto hrozbám.

Směrnice o ochraně údajů policií a trestním soudnictvím chrání osobní údaje různých kategorií jednotlivců, kteří jsou účastníky trestního řízení, jako jsou svědci, informátoři, oběti, podezřelí a spolupachatelé. Policejní orgány a orgány trestního soudnictví jsou povinny postupovat v souladu s ustanovením směrnice, kdykoliv zpracovávají tyto osobní údaje pro účely prosazování práva v rámci osobní i věcné působnosti směrnice.[745]

Rovněž je za určitých okolností povoleno používání údajů za jiným účelem. Zpracování údajů pro jiný účel prosazování práva, než je ten, pro který byly shromážděny, je povolen, pouze pokud je to zákonné, nezbytné a přiměřené podle vnitrostátního práva a práva EU.[746] Pro jiné účely se použijí pravidla obecného nařízení o ochraně osobních údajů. Vedení logů a dokumentování sdílení údajů je jednou ze zvláštních povinností příslušných orgánů a má pomoci objasnit povinnosti vyplývající ze stížností.

Příslušnými orgány působícími v oblasti policie a trestního soudnictví jsou orgány veřejné moci nebo orgány zmocněné vnitrostátním právem a veřejnou mocí

744 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, Úř. věst. 2016 L 119, s. 89 (směrnice o ochraně údajů policií a trestním soudnictvím).

745 Směrnice o ochraně údajů policií a trestním soudnictvím, čl. 2 odst. 1.

746 Tamtéž, čl. 4 odst. 2.

vykonávat funkce veřejného orgánu,[747] např. soukromé věznice.[748] Směrnice je použitelná jak pro zpracování údajů na vnitrostátní úrovni, tak pro přeshraniční zpracování mezi policejními orgány a orgány trestního soudnictví členských států, ale také na mezinárodní předání příslušnými orgány třetím zemím a mezinárodním organizacím.[749] Nevztahuje se na národní bezpečnost ani na zpracování osobních údajů orgány, institucemi a jinými subjekty EU.[750]

Směrnice do značné míry vychází ze zásad a definic uvedených v obecném nařízení o ochraně osobních údajů a zohledňuje zvláštní povahu policejního sektoru a sektoru trestního soudnictví. Dohled mohou provádět tytéž orgány členského státu, které provádějí dozor i podle obecného nařízení o ochraně osobních údajů. Do směrnice bylo jako nová povinnost pro policejní orgány a orgány trestního soudnictvím zavedeno jmenování pověřenců pro ochranu osobních údajů a provádění posouzení vlivu na ochranu osobních údajů.[751] Ačkoliv jsou tyto koncepce inspirovány obecným nařízením o ochraně osobních údajů, zabývá se směrnice zvláštní povahou policejních orgánů a orgánů trestního soudnictví. Ve srovnání se zpracováním údajů pro obchodní účely, které je upraveno nařízením, může zpracování pro bezpečnostní účely vyžadovat určitou míru flexibility. Například pokud by subjektům údajů byla poskytnuta stejná úroveň ochrany, pokud jde o právo na informace, na přístup k jejich osobním údajům či jejich výmaz, jako podle obecného nařízení o ochraně osobních údajů, mohlo by to znamenat, že by se veškeré operace sledování prováděné pro účely prosazování práva mohly stát v kontextu prosazování práva neúčinnými. Směrnice proto neobsahuje zásadu transparentnosti. Obdobně je nutné také uplatňovat při zpracování pro bezpečnostní účely flexibilitu s ohledem na zásadu minimalizace údajů a účelového omezení, které stanoví povinnost, aby osobní údaje byly omezeny na to, co je nezbytné, pokud jde o účely, pro které jsou tyto údaje zpracovávány, a aby byly zpracovávány za účelem dosažení určitých a výslovně vyjádřených cílů. Informace shromážděné a uložené příslušnými orgány ke konkrétnímu případu se mohou ukázat jako velmi užitečné při řešení budoucích případů.

747 Tamtéž, čl. 3 odst. 7.

748 Evropská komise (2016), Sdělení Komise Evropskému parlamentu podle čl. 294 odst. 6 Smlouvy o fungování Evropské unie týkající se postoje Rady k přijetí směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů, kterou se zrušuje rámcové rozhodnutí Rady 2008/977/SVV, COM(2016) 213 final, Brusel, 11. dubna 2016.

749 Směrnice o ochraně údajů policií a trestním soudnictvím, kapitola V.

750 Tamtéž, čl. 2 odst. 3.

751 Tamtéž, v článku 32, resp. článku 27.

Zásady týkající se zpracování

Směrnice o ochraně údajů policií a trestním soudnictvím stanoví určité klíčové záruky týkající se použití osobních údajů. Rovněž vyjmenovává zásady, jimiž se řídí zpracování těchto údajů. Členské státy musejí zajistit, aby osobní údaje byly:

- zpracovávány zákonným a korektním způsobem,
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nebyly zpracovávány způsobem, který je s těmito účely neslučitelný,
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány,
- přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření zajišťující, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které jsou zpracovávány, byly bezodkladně vymazány nebo opraveny,
- uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány,
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.[752]

Podle směrnice je zpracování zákonné pouze tehdy, pokud k němu dochází v míře nezbytné k plnění příslušných úkolů. Kromě toho by zpracování mělo být prováděno příslušným orgánem sledujícím cíle stanovené směrnicí a mít základ v právu EU nebo členského státu.[753] Údaje nesmějí být uchovávány po dobu delší, než je nezbytné, a musejí být vymazány nebo v určitých lhůtách pravidelně přezkoumány. Musí je používat pouze příslušný orgán a pro účely, pro které byly tyto údaje shromážděny, předány nebo zpřístupněny.

752 Tamtéž, čl. 4 odst. 1.

753 Tamtéž, článek 8.

Práva subjektu údajů

Směrnice rovněž stanoví práva subjektu údajů. Patří k nim:

- Právo na informace. Členské státy musí uložit správci údajů povinnost zpřístupnit subjektu údajů: 1) údaje o totožnosti a kontaktní údaje správce, 2) kontaktní údaje pověřence pro ochranu osobních údajů, 3) účely zpracování, pro které jsou osobní údaje určeny, 4) právo podat stížnost u příslušného dozorovému úřadu a kontaktní údaje tohoto úřadu a 5) právo na přístup k osobním údajům, jejich opravu nebo výmaz anebo omezení jejich zpracování.[754] Vedle těchto obecných požadavků na informace směrnice stanoví, že ve zvláštních případech musí správci subjektům údajů poskytnout informace o právním základu zpracování a o tom, jak dlouho budou údaje uloženy, s cílem umožnit výkon jejich práv. Pokud jsou osobní údaje předány jiným příjemcům, mimo jiné do třetích zemí a mezinárodním organizacím, musejí být subjekty údajů informovány o kategoriích těchto příjemců. V neposlední řadě musí správce poskytnout veškeré další informace s ohledem na zvláštní okolnosti, za kterých jsou údaje zpracovávány – například pokud byly osobní údaje shromážděny během tajného sledování, tj. bez vědomí subjektu údajů. Tím se zaručí korektní zpracování vzhledem k subjektu údajů.[755]

- Právo na přístup k osobním údajům. Členské státy musí zajistit, aby měl subjekt údajů právo dozvědět se, zda jeho osobní údaje jsou či nejsou zpracovávány. Pokud jsou, měl by mít subjekt údajů přístup k určitým informacím, jako jsou kategorie zpracovávaných údajů.[756] Avšak toto právo může být omezeno – například s cílem zabránit maření vyšetřování nebo zabránit nepříznivému ovlivňování stíhání trestné činnosti nebo s cílem chránit veřejnou bezpečnost a práva a svobody druhých.[757]

- Právo na opravu osobních údajů. Členské státy jsou povinny zajistit, aby subjekt údajů mohl bez zbytečného odkladu dosáhnout opravy nepřesných osobních údajů. Dále má subjekt údajů právo na doplnění neúplných osobních údajů.[758]

754 Tamtéž, čl. 13 odst. 1.

755 Tamtéž, čl. 13 odst. 2.

756 Tamtéž, článek 14.

757 Tamtéž, článek 15.

758 Tamtéž, čl. 16 odst. 1.

- Právo na výmaz osobních údajů a omezení zpracování. V určitých případech musí správce osobní údaje smazat. Kromě toho může dosáhnout výmazu svých osobních údajů subjekt údajů, ale pouze pokud jsou tyto údaje zpracovávány protiprávně.[759] V určitých situacích může být namísto výmazu zpracování osobních údajů omezeno. K tomu může dojít v situaci, kdy 1) je zpochybněna přesnost osobního údaje a nelze jej ověřit nebo 2) jsou osobní údaje nezbytné pro účely dokazování.[760]

Kdykoliv správce odmítne provést opravu nebo výmaz osobních údajů nebo omezit zpracování údajů, musí být subjekt údajů o tomto rozhodnutí písemně informován. Členské státy mohou toto právo omezit kromě jiného za účelem ochrany veřejné bezpečnosti nebo práv a svobod jiných osob, a to z týchž důvodů, které platí pro omezení práva na přístup.[761]

Subjekt údajů má obvykle nárok na informace o zpracování svých osobních údajů a má právo na přístup, opravu nebo výmaz omezení zpracování, které může sám uplatňovat přímo u správce. Jako záložní řešení je také možné podle směrnice o ochraně údajů policií a trestním soudnictvím nepřímé uplatňování práv subjektu údajů prostřednictvím jeho dozorového úřadu v oblasti ochrany údajů a toto záložní řešení se použije, pokud správce omezuje právo subjektu údajů.[762] Článek 17 směrnice ukládá členským státům povinnost přijmout opatření, která zajistí, aby práva subjektů údajů bylo možné vykonávat rovněž prostřednictvím jejich dozorového úřadu. Proto musí správce údajů informovat subjekt údajů o možnosti nepřímého přístupu.

Povinnosti správce a zpracovatele

V kontextu směrnice o ochraně údajů policií a trestním soudnictvím jsou správci údajů příslušné orgány veřejné moci nebo jiné subjekty s příslušnými veřejnými pravomocemi a veřejnou mocí, které určují účely a prostředky zpracování osobních údajů. Směrnice stanoví několik povinností pro správce údajů, aby byla zajištěna vysoká úroveň ochrany osobních údajů zpracovaných pro účely prosazování práva.

759 Tamtéž, čl. 16 odst. 2.

760 Tamtéž, čl. 16 odst. 3.

761 Tamtéž, čl. 16 odst. 4.

762 Tamtéž, článek 17.

Příslušné orgány musí vést logy pro operace zpracování, které provádějí v rámci automatizovaných systémů zpracování. Logy musí být vedeny alespoň pro shromažďování, pozměňování, nahlížení, sdělování včetně předávání, kombinování nebo výmazu osobních údajů.[763] Směrnice stanoví, že logy o nahlédnutí a sdělení musí umožňovat zjištění data a času operací, jejich důvodů, a je-li to možné, totožnosti osoby, která do systému nahlédla nebo která osobní údaje zpřístupnila, a příjemců dotčených osobních údajů. Logy se musejí používat pouze za účelem ověření zákonnosti zpracování, vlastní kontroly, pro zajištění neporušenosti a zabezpečení osobních údajů a pro trestní řízení.[764] Na žádost dozorového úřadu musí správce a zpracovatel tomuto úřadu logy zpřístupnit.

Zejména platí pro správce a zpracovatele obecná povinnost zavést vhodná technická a organizační opatření, aby bylo zajištěno, že zpracování se provádí v souladu se směrnicí, a být schopen prokázat zákonnost takového zpracování.[765] Při návrhu těchto opatření musejí přihlédnout k povaze, rozsahu, kontextu zpracování a zejména k veškerým případným rizikům pro práva a svobody jednotlivců. Správci by měli přijmout vnitřní koncepce a zavést opatření, která usnadňují dodržování zásad ochrany údajů, zejména zásady záměrné a standardní ochrany osobních údajů.[766] Pokud je pravděpodobné, že zpracování bude mít za následek vysoké riziko pro práva jednotlivců – například kvůli použití nových technologií – musí správci provést před zahájením zpracování posouzení vlivu na ochranu osobních údajů.[767] Směrnice také vyjmenovává opatření, která musí správci provést, aby zajistili bezpečnost zpracování. K nim patří opatření s cílem zabránit neoprávněnému přístupu k jimi zpracovávaným osobních údajům, zajistit, aby oprávněné osoby měly přístup pouze k osobním údajům, na které se vztahuje jejich povolení k přístupu, zajistit, aby systém zpracování řádně fungoval a aby uložené osobní údaje nebylo možné poškodit špatným fungováním systému.[768] Pokud dojde k porušení zabezpečení osobních údajů, musí správci do tří dnů uvědomit dozorový úřad, popsat povahu porušení, jeho pravděpodobné důsledky, kategorie dotčených osobních údajů a přibližný počet příslušných dotčených subjektů údajů. Porušení zabezpečení osobních údajů musí být také oznámeno „bez zbytečného odkladu" subjektu údajů, pokud je

763 Tamtéž, čl. 25 odst. 1.

764 Tamtéž, čl. 25 odst. 2.

765 Tamtéž, článek 19.

766 Tamtéž, článek 20.

767 Tamtéž, článek 27.

768 Tamtéž, článek 29.

pravděpodobné, že porušení bude mít za následek vysoké riziko pro jeho práva a svobody.[769]

Směrnice obsahuje zásadu odpovědnosti a ukládá správcům povinnost provádět opatření k zajištění souladu s touto zásadou. Správci musí vést záznamy o všech kategoriích činností zpracování, za které nesou odpovědnost: podrobný obsah těchto záznamů je upřesněn v článku 24 směrnice. Záznamy musí být k dispozici dozorovému úřadu na vyžádání, aby mohly tyto úřady monitorovat operace zpracování daného správce. Dalším důležitým opatřením k posílení odpovědnosti je jmenování pověřence pro ochranu osobních údajů. Správci musejí jmenovat pověřence pro ochranu osobních údajů, ačkoliv směrnice členským státům umožňuje vynětí soudů a jiných nezávislých justičních orgánů z této povinnosti.[770] Povinnosti pověřence pro ochranu osobních údajů připomínají povinnosti pověřenců podle obecného nařízení o ochraně osobních údajů. Monitoruje dodržování směrnice a poskytuje informace a poradenství zaměstnancům, kteří provádějí zpracování údajů, o jejich povinnostech podle právních předpisů v oblasti ochrany údajů. Pověřenec pro ochranu osobních údajů rovněž poskytuje poradenství ohledně nutnosti provádět posouzení vlivu na ochranu osobních údajů a působí jako kontaktní místo pro dozorový úřad.

Předávání do třetích zemí nebo mezinárodním organizacím

Směrnice, podobně jako obecné nařízení o ochraně osobních údajů, stanoví podmínky pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím. Pokud by byly osobní údaje svobodně předány mimo jurisdikci EU, mohly by být ohroženy záruky a silná ochrana, kterou stanoví právo EU. Samotné podmínky se však velmi liší od podmínek uvedených v obecném nařízení o ochraně osobních údajů. Předání osobních údajů do třetích zemí nebo mezinárodním organizacím je povoleno, pokud:[771]

- Předání je nezbytné pro dosažení cílů směrnice.

- Osobní údaje se předávají příslušnému orgánu třetí země nebo mezinárodní organizace ve smyslu definice uvedené ve směrnici – ačkoliv je stanovena výjimka z tohoto pravidla v individuálních a zvláštních případech.[772]

769 Tamtéž, články 30 a 31.

770 Tamtéž, článek 32.

771 Tamtéž, článek 35.

772 Tamtéž, článek 39.

- Předávání osobních údajů, které byly přijaty v rámci přeshraniční spolupráce, do třetích zemí nebo mezinárodním organizacím vyžaduje povolení členského státu, ze kterého údaje pocházejí, ačkoliv v naléhavých případech jsou stanoveny výjimky.

- Evropská komise přijala rozhodnutí o odpovídající ochraně, byly stanoveny vhodné záruky nebo se použije výjimka pro předávání v konkrétních situacích.

- Další předávání osobních údajů do jiné třetí země nebo mezinárodní organizaci vyžaduje předchozí povolení příslušného orgánu původu, které kromě jiného zohlední závažnost trestného činu a úroveň ochrany údajů v zemi určení druhého mezinárodního předání.[773]

Podle směrnice může k předávání osobních údajů dojít, pokud je splněna jedna ze tří podmínek. První podmínkou je, že Evropská komise vydala rozhodnutí o odpovídající ochraně podle směrnice. Rozhodnutí se může vztahovat na celé území třetí země nebo na určitá odvětví třetí země nebo na mezinárodní organizaci. To však je možné, pouze pokud je zajištěna odpovídající úroveň ochrany a jsou splněny podmínky uvedené ve směrnici.[774] V takových případech předání osobních údajů nepodléhá povolení členského státu.[775] Evropská komise musí sledovat vývoj, který by mohl ovlivnit fungování rozhodnutí o odpovídající ochraně. Navíc musí rozhodnutí zahrnovat mechanismus pro pravidelný přezkum. Komise také může zrušit, změnit anebo pozastavit účinnost rozhodnutí, pokud z dostupných informací vyplyne, že podmínky ve třetí zemi nebo mezinárodní organizaci již nezajišťují odpovídající úroveň ochrany. V takovém případě musí Komise zahájit konzultace s danou třetí zemí nebo mezinárodní organizací a pokusit se o nápravu situace.

Pokud není vydáno rozhodnutí o odpovídající ochraně, může být předání založeno na vhodných zárukách. Ty mohou být stanoveny v právně závazném nástroji nebo může správce provádět vlastní hodnocení okolností, na jejichž pozadí k předání osobních údajů dochází, a může dospět k závěru, že existují vhodné záruky. Vlastní hodnocení by mělo vzít v úvahu i možné dohody o spolupráci uzavřené mezi Europolem a Eurojustem a třetí zemí nebo mezinárodní organizací, existenci povinnosti související se zachováním mlčenlivosti a omezení účelu, jakož i poskytnuté záruky, že údaje nebudou použity v souvislosti s jakoukoli formou krutého

773 Tamtéž, čl. 35 odst. 1.

774 Tamtéž, článek 36.

775 Tamtéž, čl. 36 odst. 1.

a nelidského zacházení, včetně trestu smrti.[776] V posledním uvedeném případě musí správce informovat příslušný dozorový úřad o kategoriích předání spadajících do této kategorie.[777]

I přestože nebylo přijato rozhodnutí o odpovídající ochraně ani nebyly poskytnuty vhodné záruky, může být předání možné v určitých situacích uvedených ve směrnici. Patří k nim mimo jiné ochrana životně důležitých zájmů subjektu údajů nebo jiné osoby a zabránění bezprostřednímu a závažnému ohrožení veřejné bezpečnosti v určitém členském státě nebo třetí zemi.[778]

V individuálních a zvláštních případech může dojít k předání údajů ze strany příslušných orgánů příjemcům usazeným ve třetích zemích, které nejsou příslušnými orgány, pokud jsou kromě jedné ze tří podmínek uvedených výše splněny i další podmínky stanovené v článku 39 směrnice. Zejména pak musí být předání naprosto nezbytné pro plnění úkolu předávajícího příslušného orgánu, který je také zodpovědný za určení, že veřejnému zájmu, který předání odůvodňuje, nejsou nadřazena základní práva a svobody jednotlivce. Takové předání musí být zdokumentováno a předávající příslušný orgán musí informovat příslušný dozorový úřad.[779]

V neposlední řadě směrnice také ukládá ve vztahu ke třetím zemím a mezinárodním organizacím povinnost rozvíjet mechanismy pro mezinárodní spolupráci, aby se usnadnilo účinné vymáhání právních předpisů, a tak pomáhá dozorovým úřadům v oblasti ochrany údajů spolupracovat s jejich zahraničními protějšky.[780]

Nezávislý dohled a ochrana subjektů údajů

Každý členský stát musí zajistit, aby jeden nebo více nezávislých dozorových úřadů byl odpovědný za poradenství a monitorování uplatňování příslušných ustanovení přijatých podle uvedené směrnice.[781] Dozorový úřad zřízený pro účely směrnice může být totožný s dozorovým úřadem zřízeným podle obecného nařízení o ochraně osobních údajů, ale členské státy mohou podle vlastního uvážení jmenovat jiný úřad, pokud jsou splněna kritéria nezávislosti. Na dozorové úřady se rovněž

776 Tamtéž, 71. bod odůvodnění.

777 Tamtéž, čl. 37 odst. 1.

778 Tamtéž, čl. 38 odst. 1.

779 Tamtéž, čl. 37 odst. 3.

780 Tamtéž, článek 40.

781 Tamtéž, článek 41.

může každá osoba obrátit se stížností týkající se ochrany jejích práv a svobod, pokud jde o zpracování osobních údajů příslušnými orgány.

Pokud je výkon práv subjektu údajů odmítnut z pádných důvodů, musí mít subjekt údajů právo na odvolání k příslušnému vnitrostátnímu dozorovému úřadu a/nebo k soudu. Pokud určitá osobu v důsledku porušení vnitrostátních právních předpisů provádějících tuto směrnici utrpí újmu, má právo na náhradu od správce nebo jakéhokoliv jiného orgánu příslušného podle práva členského státu.[782] Obecně platí, že subjekty údajů musí mít přístup k soudní ochraně, pokud jde o každé porušení jejich práv zaručených vnitrostátními právními předpisy provádějícími uvedenou směrnici.[783]

8.3. Jiné zvláštní právní nástroje v oblasti ochrany údajů ve věcech týkajících se prosazování práva

Kromě směrnice o ochraně údajů policií a trestním soudnictvím je výměna informací ve vlastnictví členských států v určitých oblastech upravena řadou právních nástrojů – například rámcovým rozhodnutím Rady 2009/315/SVV o organizaci a obsahu výměny informací z rejstříku trestů mezi členskými státy, rozhodnutím Rady 2000/642/SVV o způsobech spolupráce mezi finančními zpravodajskými jednotkami členských států při výměně informací a rámcovým rozhodnutím Rady 2006/960/SVV ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie.[784]

Je důležité připomenout, že přeshraniční spolupráce[785] mezi příslušnými orgány stále více zahrnuje výměnu údajů o přistěhovalectví. Tato oblast práva se nepovažuje

782 Tamtéž, článek 56.

783 Tamtéž, článek 54.

784 Rada Evropské unie (2009), rámcové rozhodnutí Rady 2009/315/SVV ze dne 26. února 2009 o organizaci a obsahu výměny informací z rejstříku trestů mezi členskými státy, Úř. věst. 2009 L 93; Rada Evropské unie (2000), rozhodnutí Rady 2000/642/SVV ze dne 17. října 2000 o způsobech spolupráce mezi finančními zpravodajskými jednotkami členských států při výměně informací, Úř. věst. 2000 L 271; rámcové rozhodnutí Rady 2006/960/SVV ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie, Úř. věst. L 386.

785 Evropská komise (2012), *Sdělení Komise Evropskému parlamentu a Radě – Posílení spolupráce při prosazování práva v EU: Evropský model pro výměnu informací (EIXM)*, COM(2012) 735 final, Brusel, 7. prosince 2012.

za součást věcí týkajících se policie a trestního soudnictví, ale je v mnoha ohledech relevantní pro práci policie a soudních orgánů. Totéž platí i o údajích o zboží dováženém do EU i vyváženém z EU. Odstranění kontrol na vnitřních hranicích v rámci schengenského prostoru zvýšilo riziko podvodů. Je tudíž nezbytné, aby členské státy posílily spolupráci, zejména zlepšením přeshraniční výměny informací, aby mohly účinněji odhalovat a stíhat případy porušení celních právních předpisů členských států i EU. Kromě toho došlo v uplynulých letech ve světě k nárůstu závažné a organizované trestné činnosti a terorismu, která může zahrnovat mezinárodní cestování, a byla v mnoha případech odhalena nutnost posílené přeshraniční spolupráce ze strany policie a donucovacích orgánů.[786]

Prümské rozhodnutí

Důležitým příkladem interinstitucionální přeshraniční spolupráce formou výměny údajů ve vlastnictví jednotlivých států je rozhodnutí Rady 2008/615/SVV spolu s jeho prováděcími ustanoveními v rozhodnutí 2008/615/SVV o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (prümské rozhodnutí), kterým se v roce 2008 začlenila do práva EU Prümská smlouva.[787] Prümská smlouva byla dohoda o mezinárodní policejní spolupráci podepsaná v roce 2005 Belgií, Francií, Lucemburskem, Německem, Nizozemskem, Rakouskem a Španělskem.[788]

Cílem prümského rozhodnutí je pomoci signatářským členským státům zlepšit sdílení informací za účelem předcházení trestné činnosti a boje proti ní ve třech oblastech: terorismu, přeshraniční trestné činnosti a nedovolené migraci. Za tímto účelem rozhodnutí obsahuje ustanovení týkající se:

- automatizovaného přístupu k profilům DNA, údajům o otiscích prstů a některým vnitrostátním údajům o registraci vozidel,

786 Viz Evropská komise (2011), Návrh směrnice Evropského parlamentu a Rady o používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti, KOM(2011) 32 final, Brusel, 2. února 2011, s. 1.

787 Rada Evropské unie (2008), Rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti, Úř. věst. 2008 L 210.

788 Smlouva mezi Belgickým královstvím, Spolkovou republikou Německo, Španělským královstvím, Francouzskou republikou, Lucemburským velkovévodstvím, Nizozemským královstvím a Rakouskou republikou o posílení přeshraniční spolupráce, zejména v boji proti terorismu, přeshraniční trestné činnosti a nedovolené migraci.

- dodání údajů v souvislosti s významnými událostmi, které mají přeshraniční rozměr,

- dodání informací za účelem zabránění teroristickým trestným činům,

- jiných opatření na posílení přeshraniční policejní spolupráce.

Databáze zpřístupněné podle prümského rozhodnutí se řídí v plné míře vnitrostátním právem, ale výměna údajů je navíc upravena rozhodnutím, jehož slučitelnost se směrnicí o ochraně údajů policií a trestním soudnictvím bude muset být posouzena. Příslušnými subjekty pro dohled nad těmito pohyby údajů jsou vnitrostátní dozorové úřady v oblasti ochrany údajů.

Rámcové rozhodnutí 2006/960/SVV – švédská iniciativa

Rámcové rozhodnutí 2006/960/SVV (švédská iniciativa)[789] představuje jiný příklad přeshraniční spolupráce s ohledem na výměnu údajů ve vlastnictví donucovacích orgánů na vnitrostátní úrovni. Švédská iniciativa se výslovně zaměřuje na výměnu operativních a jiných informací a stanoví zvláštní pravidla ochrany údajů, a sice v článku 8.

Podle tohoto nástroje se musí použití vyměňovaných operativních a jiných informací řídit vnitrostátními ustanoveními na ochranu údajů členského státu, který informace přijímá, a to podle týchž pravidel, jako kdyby byly tyto informace získány v daném členském státě. Článek 8 zachází ještě dál a uvádí se zde, že při poskytování operativních a jiných informací může příslušný donucovací orgán podle svého vnitrostátního práva uložit příslušnému přijímajícímu donucovacímu orgánu podmínky pro použití těchto informací. Tyto podmínky se mohou též vztahovat na oznamování výsledků vyšetřování trestné činnosti nebo operativně pátrací činnosti, v jejichž rámci byla výměna operativních nebo jiných informací nutná. Pokud však vnitrostátní právo stanoví odchylky od omezení použití (např. pro justiční orgány, zákonodárné orgány atd.), mohou být operativní a jiné informace použity pouze po předchozí konzultaci s předávajícím členským státem.

Poskytnuté operativní a jiné informace mohou být použity:

789 Rada Evropské unie (2006), Rámcové rozhodnutí Rady 2006/960/SVV ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie, Úř. věst. L 386/89 ze dne 29. prosince 2006.

- pro účely, ke kterým byly poskytnuty, nebo
- k zabránění bezprostřednímu a vážnému ohrožení veřejné bezpečnosti.

Zpracování pro jiné účely je přípustné pouze s předchozím povolením předávajícího členského státu.

Švédská iniciativa dále uvádí, že zpracovávané osobní údaje musí být chráněny v souladu s mezinárodními nástroji, jako je:

- Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat,[790]
- Dodatkový protokol ze dne 8. listopadu 2001 k této úmluvě o dozorčích orgánech a toku údajů přes hranice,[791]
- Doporučení Rady Evropy č. R(87) 15 upravující používání osobních údajů v policejním sektoru.[792]

Směrnice EU o jmenné evidenci cestujících

Údaje ze jmenné evidence cestujících se týkají informací o cestujících v letecké dopravě, které jsou shromážděny a uvedeny v rezervačních systémech a kontrolních systémech odletů užívaných přepravci pro vlastní komerční účely. Tyto údaje obsahují několik různých druhů informací, jako jsou termíny cest, cestovní itinerář, informace o letenkách, kontaktní údaje, cestovní zprostředkovatel, přes nějž byl let rezervován, použitý způsob platby, čísla sedadel a údaje o zavazadlech.[793] Zpracování údajů jmenné evidence cestujících může pomoci donucovacím orgánům určit známé nebo potenciální podezřelé osoby a provádět hodnocení založená na cestovních návycích a jiných ukazatelích, které jsou obvykle spojeny s trestnou činností. Analýza údajů jmenné evidence cestujících rovněž umožňuje zpětné sledování cest

790 Rada Evropy (1981), Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat, ETS č. 108.

791 Rada Evropy (2001), Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o dozorčích orgánech a toku údajů přes hranice, ETS č. 108.

792 Rada Evropy (1987), Doporučení Výboru ministrů č. R (87) 15 členským státům upravující používání osobních údajů v policejním sektoru (přijaté Výborem ministrů dne 17. září 1987 na 410. zasedání náměstků ministrů).

793 Evropská komise (2011), Návrh směrnice Evropského parlamentu a Rady o používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti, KOM(2011) 32 final, Brusel, 2. února 2011, s. 1.

a kontaktů osob podezřelých z účasti na trestné činnosti, což může umožnit donucovacím orgánům odhalit zločinecké sítě.[794] Za účelem výměny údajů o jmenné evidenci cestujících uzavřela EU určité dohody se třetími zeměmi, jak je vysvětleno v oddíle 7. Kromě toho zavedla zpracování údajů jmenné evidence cestujících v rámci EU prostřednictvím směrnice (EU) 2016/681 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti (směrnice EU o jmenné evidenci cestujících).[795] Tato směrnice stanoví povinnosti leteckých dopravců předávat údaje jmenné evidence cestujících příslušným orgánům a stanovit důsledné záruky ochrany údajů pro zpracování a shromažďování těchto údajů. Směrnice EU o jmenné evidenci cestujících se vztahuje na mezinárodní lety do EU a z EU, ale také na lety v rámci EU, pokud se tak daný členský stát rozhodne.[796]

Údaje jmenné evidence cestujících musí obsahovat pouze informace, které povoluje směrnice EU o jmenné evidenci cestujících. Musí být uchovávány v jediném útvaru pro informace nacházejícím se na zabezpečeném místě v každém členském státě. Údaje jmenné evidence cestujících musí být každých šest měsíců po předání leteckým dopravcem depersonalizovány a uchovávány po dobu nejvýše pěti let.[797] Údaje jmenné evidence cestujících se vyměňují mezi členskými státy, mezi členskými státy a Europolem a se třetími zeměmi, ale pouze v jednotlivých případech.

Předání a zpracování údajů jmenné evidence cestujících a práv zaručených subjektům údajů musí být v souladu se směrnicí o ochraně údajů policií a trestním soudnictvím a musí zajišťovat vysokou úroveň ochrany soukromí a osobních údajů, jak ukládá Listina, Modernizovaná úmluva č. 108 a EÚLP.

Nezávislé vnitrostátní dozorové úřady, které jsou příslušné podle směrnice o ochraně údajů policií a trestním soudnictvím, jsou také odpovědné za poradenství ohledně ustanovení přijatých členskými státy podle směrnice EU o jmenné evidenci cestujících, jakož i za sledování provádění těchto ustanovení.

794 Evropská komise (2015), Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives [Informativní přehled – boj proti terorismu na úrovni EU, přehled činností, opatření a iniciativ Komise], Brusel, 11. ledna 2015.

795 Směrnice Evropského parlam entu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti, Úř. věst. 2016 L 119, s. 132.

796 Směrnice o jmenné evidenci cestujících, L 119, s. 132, čl. 1 odst. 1 a čl. 2 odst. 1.

797 Tamtéž, čl. 12 odst. 1 a čl. 12 odst. 2.

Uchovávání údajů o telekomunikacích

Směrnice o uchovávání údajů[798] – která byla dne 8. dubna 2014 prohlášena za neplatnou ve věci *Digital Rights Ireland* – ukládala poskytovatelům komunikačních služeb povinnost uchovávat metadata dostupná za zvláštním účelem boje proti závažné trestné činnosti po dobu nejméně šesti, ale ne více než 24 měsíců, bez ohledu na to, zda poskytovatel stále tyto údaje potřebuje pro účely účtování nebo k technickému poskytování služby.

Uchovávání údajů o telekomunikacích jasně zasahuje do práva na ochranu údajů.[799] Zda je tento zásah odůvodněný či nikoliv, bylo napadeno v rámci několika soudních řízení v členských státech EU.[800]

Příklad: Ve věci *Digital Rights Ireland* a *Kärntner Landesregierung a další*[801] podala skupina Digital Rights žalobu u vrchního soudu (High Court) v Irsku a pan Seitlinger u ústavního soudu v Rakousku, ve které napadli legalitu vnitrostátních opatření, která umožňují uchovávání údajů elektronické komunikace. Skupina Digital Rights požádala irský soud, aby prohlásil směrnici 2006/24 a část vnitrostátního trestního zákona související s teroristickými trestnými činy za neplatnou. Podobně pan Seitlinger a více než 11 000 dalších účastníků napadli a požádali o prohlášení neplatnosti ustanovení rakouského zákona o telekomunikacích, kterým se prováděla směrnice 2006/24.

Při projednávání těchto žádostí o rozhodnutí o předběžné otázce SDEU prohlásil směrnici o uchovávání údajů za neplatnou. Podle SDEU poskytovaly údaje, které mohly být uchovávány podle této směrnice, jako celek přesné informace o jednotlivcích. Kromě toho přezkoumal SDEU závažnost zásahu do

798 Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. 2006 L 105.

799 EIOÚ (2011), *Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) [Stanovisko ze dne 31. května 2011 k hodnotící zprávě Komise Radě a Evropskému parlamentu o směrnici o uchovávání údajů (směrnice 2006/24/ES)]*, 31. května 2011.

800 Německo, Spolkový ústavní soud (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. března 2010; Rumunsko, Federální ústavní soud (*Curtea Constituțională a României*), č. 1258, 8. října 2009; Česká republika, Ústavní soud (Ústavní soud České republiky), 94/2011 Sb., 22. března 2011.

801 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další* a Kärntner Landesregierung a další, bod 65.

základního práva na respektování soukromého života a na ochranu osobních údajů. Došel k závěru, že uchovávání uspokojuje cíl veřejného zájmu – konkrétně boj proti závažné trestné činnosti, a tudíž veřejnou bezpečnost. SDEU přesto konstatoval, že normotvůrce EU tím, že přijal tuto směrnici, jednal v rozporu se zásadou proporcionality. Ačkoliv směrnice může být vhodná k dosažení požadovaného cíle, „velmi rozsáhlý a zvlášť závažný zásah [této směrnice] do těchto základních práv na respektování soukromí a ochranu osobních údajů není dostatečně vymezen, aby bylo zaručeno, že je zásah skutečně omezen na nezbytné minimum".

Pokud neexistuje zvláštní právní předpis týkající se uchovávání, je uchovávání údajů přípustné jako výjimka z povinnosti zachovávat důvěrný charakter telekomunikačních údajů podle směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích)[802], jako preventivní opatření, ale musí být vyhrazena výlučně pro boj proti závažné trestné činnosti. Toto uchovávání musí být omezeno na to, co je naprosto nezbytné s ohledem na kategorie uchovávaných údajů, dotčené prostředky komunikace, dotčené osoby a zvolenou dobu trvání, po kterou se údaje uchovávají. Vnitrostátní orgány mohou mít přístup k uchovávaným údajům za přísných podmínek, včetně předchozí kontroly nezávislým orgánem. Údaje musí být uchovávány v rámci EU.

Příklad: V návaznosti na rozsudky *Digital Rights Ireland* a *Kärntner Landesregierung a další*[803] byly předloženy SDEU dvě další věci týkající se obecné povinnosti ukládané ve Švédsku a ve Spojeném království poskytovatelům služeb elektronické komunikace s cílem uchovávat údaje o telekomunikacích, jak stanovila zneplatněná směrnice o uchovávání údajů. Ve věcech *Tele2 Sverige* a *Home Department v. Tom Watson a další*[804] SDEU rozhodl, že vnitrostátní právní předpisy, které stanoví obecné a neomezené uchovávání údajů, aniž by bylo zapotřebí souvislosti mezi údaji, které musejí být uchovávány, a hrozby pro veřejnou bezpečnost a aniž by byly upřesněny jakékoliv

802 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. 2002 L 201.

803 Rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*.

804 Rozsudek SDEU (velkého senátu) ze dne 21. prosince 2016, spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Tom Watson a další*.

podmínky – např. časová lhůta pro uchovávání, zeměpisná oblast, skupina osob, u nichž je pravděpodobné, že se budou účastnit trestné činnosti –, překračuje omezení toho, co je naprosto nezbytné, a nelze je považovat za odůvodněné v demokratické společnosti, jak ukládá směrnice 2002/58/ES ve spojení s Listinou základních práv EU.

Budoucnost

V lednu 2017 zveřejnila Evropská komise návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES.[805] Návrh neobsahuje žádná konkrétní ustanovení o uchovávání údajů. Stanoví však, že členské státy mohou právním předpisem omezit některé povinnosti a práva, jestliže takové omezení představuje nezbytné a přiměřené opatření na ochranu konkrétních veřejných zájmů, včetně národní bezpečnosti, obrany, veřejné bezpečnosti, předcházení trestným činům a jejich vyšetřování, odhalování či stíhání nebo výkonu trestů.[806] Proto členské státy byly schopny zachovat nebo vytvořit vnitrostátní rámce pro uchovávání údajů, které stanoví cílená opatření pro uchovávání údajů, pokud jsou tyto rámce v souladu s právem Unie a zohledňují judikaturu Soudního dvora týkající se výkladu směrnice o soukromí a elektronických komunikacích a Listiny základních práv.[807] V době psaní této příručky stále probíhaly diskuse o přijetí nařízení.

Zastřešující dohoda mezi EU a USA o ochraně osobních informací vyměněných za účelem prosazování práva

Dne 1. února 2017 nabyla účinnosti zastřešující dohoda mezi EU a USA o zpracovávání osobních údajů za účelem prevence, vyšetřování, odhalování a stíhání trestných činů.[808] Cílem zastřešující dohody mezi EU a USA je zajistit občanům EU vysokou úroveň ochrany údajů a současně posílit spolupráci donucovacích orgánů EU a USA. Doplňuje stávající dohody mezi donucovacími orgány EU a USA a orgány jednotlivých členských států a USA a zároveň také pomáhá zavést jasná a harmonizovaná

805 Evropská komise (2017), *Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)*, COM(2017) 10 final, Brusel, 10. ledna 2017.

806 Tamtéž, 26. bod odůvodnění.

807 Viz důvodovou zprávu k návrhu nařízení o soukromí a elektronických komunikacích COM(2017) 10 final, bod 1.3.

808 Viz Rada EU (2016), *„Posílená práva občanů EU, pokud jde o ochranu údajů, v rámci spolupráce v oblasti prosazování práva: EU a USA podepíší „zastřešující dohodu""*, Tisková zpráva 305/16, 2. června 2016.

pravidla ochrany údajů pro budoucí dohody v této oblasti. V této souvislosti je cílem dohody stanovit trvalý právní rámec, který usnadní výměnu informací.

Dohoda sama o sobě nestanoví vhodný právní základ pro výměnu osobních údajů, ale naopak nabízí vhodné záruky ochrany údajů pro dotčené jednotlivce. Vztahuje se na veškeré zpracování osobních údajů nezbytných pro účely prevence, odhalování, vyšetřování a stíhání trestných činů, včetně terorismu.[809]

Dohoda stanoví vícero záruk, které zajišťují, aby byly osobní údaje používány pouze pro účely stanovené v této dohodě. Zejména stanoví následující ochranu občanů EU:

- omezení použití údajů: osobní údaje mohou být použity pouze pro účel prevence, vyšetřování, odhalování a stíhání trestných činů,
- ochrana před svévolnou a neodůvodněnou diskriminací,
- další předání: veškeré další předání do jiné země mimo USA a EU nebo mezinárodní organizaci je podmíněno předchozím souhlasem příslušného orgánu země, která původně údaje předala,
- kvalita údajů: osobní údaje musí být uchovávány s ohledem na jejich přesnost, relevanci, včasnost a úplnost,
- zabezpečení zpracování: včetně oznámení o porušení zabezpečení osobních údajů,
- zpracování citlivých údajů je možné pouze při dodržení vhodných záruk v souladu s právními předpisy,
- doby uchovávání: osobní údaje nesmějí být uchovávány po dobu delší, než je nezbytné či vhodné,

809 Dohoda mezi Spojenými státy americkými a Evropskou unií o ochraně osobních informací v souvislosti s prevencí, vyšetřováním, odhalováním a stíháním trestných činů ze dne 18. května 2016, (OR.en) 8557/16, čl. 3 odst. 1. Viz také oznámení Komise o jednáních o dohodě o ochraně údajů mezi EU a USA ze dne 26. května 2010, MEMO/10/216 a tiskovou zprávu Evropské komise (2010) o vysokém standardu ochrany soukromí v dohodě o ochraně údajů mezi EU a USA ze dne 26. května 2010, IP/10/609.

- právo na přístup a ochranu: každý jednotlivec je oprávněn získat přístup ke svým osobním údajům za určitých podmínek a bude moci požádat o opravu údajů, pokud jsou nepřesné,
- automatizovaná rozhodnutí vyžadují vhodné záruky, včetně možnosti docílit lidského zásahu,
- účinný dohled, včetně spolupráce mezi orgány dohledu EU a USA, a
- soudní opravné prostředky a vykonatelnost: občané EU mají právo[810] uplatnit soudní ochranné prostředky u soudů USA, pokud jim orgány USA odepřou přístup nebo odmítnou provést opravu nebo protiprávně sdělí jejich osobní údaje.

V rámci „zastřešující dohody" byl rovněž zřízen systém pro oznamování veškerých případných porušení zabezpečení údajů příslušným dozorovým úřadům ve členském státě dotčených jednotlivců. Právní záruky stanovené dohodou zajišťují rovné zacházení s občany EU v USA, pokud dojde k porušení ochrany soukromí.[811]

8.3.1. Ochrana údajů v rámci agentur EU pro soudnictví a prosazování práva

Europol

Europol, agentura Evropské unie pro prosazování práva, má sídlo v Haagu, zatímco její národní jednotky (ENU) sídlí v jednotlivých členských státech. Europol byl založen v roce 1998. Jeho současný právní status jako instituce EU vychází z nařízení o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (nařízení

810 Zákon USA o soudních opravných prostředcích (Judicial Redress Act) nabyl účinnosti dnem podpisu prezidenta Obamy dne 24. února 2016.

811 Evropský inspektor ochrany údajů vydal k této dohodě mezi EU a USA stanovisko, v němž doporučil mimo jiné následující změny: 1) přidání „pro konkrétní účely, pro které byly předány" ke článku týkajícímu se uchovávání údajů, které již nejsou nezbytné a vhodné, 2) vyloučení hromadného předávání citlivých údajů, ke kterému může docházet. Viz Evropský inspektor ochrany údajů, Stanovisko 1/2016, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences [Předběžné stanovisko k dohodě mezi Spojenými státy americkými a Evropskou unií o ochraně osobních informací v souvislosti s prevencí, vyšetřováním, odhalováním a stíháním trestných činů]*, § 35.

o Europolu).[812] Cílem Europolu je pomoci předcházet a vyšetřovat organizovanou trestnou činnost, terorismus a jiné formy závažné trestné činnosti, které jsou vyjmenovány v příloze I nařízení o Europolu a které ohrožují dva a více členských států. Tohoto cíle dosahuje výměnou informací a tím, že působí jako středisko EU pro informace, které poskytuje analýzy zpravodajských informací a posouzení hrozeb.

Za tímto účelem zřídil Europol informační systém Europolu, který nabízí členským státům databázi pro výměnu zpravodajských a jiných informací o trestné činnosti prostřednictvím jejich národních jednotek Europolu. Informační systém Europolu může být použit ke zpřístupnění údajů, které se týkají: osob, které jsou podezřelé ze spáchání trestného činu, který spadá do oblasti působnosti Europolu, nebo osob, které byly za takovýto trestný čin odsouzeny; nebo osob, u nichž se má na základě věcných zjištění za to, že tyto trestné činy spáchají. Europol a jeho národní jednotky mohou přímo vkládat údaje do informačního systému Europolu a získávat z něho údaje. Pouze ta strana, která dané údaje vložila do systému, je může měnit, opravovat nebo mazat. Europolu mohou také poskytovat informace instituce EU, třetí země a mezinárodní organizace.

Informace, včetně osobních údajů, mohou být rovněž získány Europolem z veřejně dostupných zdrojů, jako je internet. Předání osobních údajů institucím EU je přípustné pouze tehdy, pokud je to nezbytně nutné pro plnění příslušných úkolů Europolu nebo přijímající instituce EU. Předání osobních údajů do třetích zemí nebo mezinárodním organizacím je možné, pouze pokud Evropská komise rozhodne, že dotčená země nebo mezinárodní organizace zajišťuje odpovídající úroveň ochrany údajů („rozhodnutí o odpovídající ochraně"), nebo pokud je uzavřena mezinárodní dohoda nebo dohoda o spolupráci. Europol může zpracovávat osobní údaje od soukromých subjektů nebo soukromých osob pouze za přísných podmínek, které stanoví, že tyto údaje předá národní jednotka Europolu v souladu se svým vnitrostátním právem, kontaktní místo v třetí zemi nebo mezinárodní organizace, s níž byla navázána spolupráce prostřednictvím dohody o spolupráci, nebo orgán třetí země nebo mezinárodní organizace, na něž se vztahuje rozhodnutí o odpovídající ochraně nebo s nimiž EU uzavřela mezinárodní dohodu. Veškeré výměny informací probíhají prostřednictvím aplikace sítě pro bezpečnou výměnu informací (SIENA).

812 Nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, Úř. věst. 2016 L 135, s. 53.

V reakci na nové události byla v rámci Europolu zřízena specializovaná střediska. V roce 2013 bylo v rámci Europolu zřízeno Evropské centrum pro boj proti kyberkriminalitě.[813] Středisko slouží jako centrum pro informace o kyberkriminalitě a přispívá k rychlejším reakcím v případě on-line trestné činnosti, k rozvíjení a nasazování digitálních forenzních kapacit a k poskytování osvědčených postupů ohledně vyšetřování kyberkriminality. Středisko se zaměřuje na kybernetickou trestnou činnost, která:

- je spáchána organizovanými skupinami vytvářejícími vysoké nezákonné zisky, jako jsou podvody na internetu,
- působí závažnou újmu obětem, např. pohlavní vykořisťování dětí na internetu,
- vážně poškozuje kritickou infrastrukturu či informační systémy v EU.

V lednu 2016 bylo zřízeno Evropské centrum pro boj proti terorismu, aby poskytovalo operativní podporu členským státům při vyšetřování spojených s teroristickými trestnými činy. Provádí porovnávání operativních údajů s údaji, které již Europol má k dispozici, rychle upozorňuje na finanční stopy a analyzuje veškeré dostupné údaje z vyšetřování, čímž pomáhá sestavit strukturovaný přehled teroristické sítě.[814]

V únoru 2016 bylo v návaznosti na zasedání Rady z listopadu 2015 zřízeno Evropské středisko pro boj proti převaděčství (EMSC), které má podporovat členské státy při boji proti zločineckým sítím podílejícím se na převaděčství migrantů a při jejich rozbíjení. Působí jako informační středisko podporující kanceláře regionálních jednotek EU v Katánii (Itálie) a v Pireu (Řecko), které pomáhají vnitrostátním orgánům v několika oblastech, včetně sdílení zpravodajských informací, vyšetřování trestných činů a stíhání zločineckých sítí převaděčů migrantů.[815]

813 Viz také EIOÚ (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre [Stanovisko evropského inspektora ochrany údajů ke sdělení Evropské komise Radě a Evropskému parlamentu o zřízení Evropského centra pro boj proti kyberkriminalitě]*, Brusel, 29. června 2012.

814 Viz webovou stránku Europolu o Evropském centru pro boj proti terorismu.

815 Viz webovou stránku Europolu o EMSC.

Režim ochrany údajů, který upravuje činnosti Europolu, je posílen a vychází ze zásad nařízení o ochraně údajů orgány EU[816] a je také v souladu se směrnicí o ochraně údajů policií a trestním soudnictvím, Modernizovanou úmluvou č. 108 a doporučením o policii.

Zpracování osobních údajů týkajících se obětí trestných činů, svědků či jiných osob, které mohou poskytnout informace o trestných činech, nebo osobních údajů týkajících se osob mladších 18 let je povoleno, jestliže je to nezbytně nutné a přiměřené pro předcházení trestné činnosti spadající do působnosti Europolu nebo boj proti ní.[817] Zpracovávání citlivých osobních údajů je zakázáno, ledaže je to nezbytně nutné a přiměřené pro předcházení trestné činnosti spadající do působnosti cílů Europolu nebo boj proti ní a pokud tyto údaje doplňují jiné osobní údaje, které Europol zpracovává.[818] V obou případech má k příslušným osobním údajům přímý přístup pouze Europol.[819]

Uchovávání údajů je povoleno pouze po dobu nutnou a přiměřenou a další uchovávání je podmíněno přezkumem, který se provádí každé tři roky, a pokud k němu nedojde, údaje se automaticky smažou.[820]

Europol může za jistých podmínek předat osobní údaje přímo subjektu EU nebo orgánu třetí země nebo mezinárodní organizaci.[821] Pokud je pravděpodobné, že porušení ochrany osobních údajů závažně a nepříznivě ovlivní práva a svobody dotčených subjektů údajů, musí být subjekty o daném porušení bez zbytečného odkladu vyrozuměny.[822] Na úrovni členských států bude jmenován vnitrostátní dozorový úřad, který bude sledovat zpracovávání osobních údajů ze strany Europol.[823]

EIOÚ odpovídá za kontrolu a uplatňování ustanovení tohoto nařízení týkajících se ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním

816 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

817 Nařízení o Europolu, čl. 30 odst. 1.

818 Tamtéž, čl. 30 odst. 2.

819 Tamtéž, čl. 30 odst. 3.

820 Tamtéž, článek 31.

821 Tamtéž, článek 24, resp. článek 25.

822 Tamtéž, článek 35.

823 Nařízení o Europolu, článek 42.

osobních údajů Europolem a za poskytování poradenství Europolu a subjektům údajů ve všech záležitostech týkajících se zpracování osobních údajů. Za tímto účelem EIOÚ vyšetřuje a přijímá stížnosti a postupuje v úzké spolupráci s vnitrostátními dozorovými úřady.[824] EIOÚ a vnitrostátní dozorové úřady se setkávají nejméně dvakrát ročně na zasedání rady spolupráce, která plní poradní funkci.[825] Členské státy jsou povinny zákonem určit vnitrostátní dozorový úřad, který je příslušný dohlížet na přípustnost předávání osobních údajů příslušným členským státem Europolu a vyhledávání a sdělování osobních údajů Europolu ze strany členských států.[826] Členské státy jsou také povinny zajistit, aby vnitrostátní dozorové úřady jednaly při výkonu svých úkolů a povinností podle nařízení o Europolu zcela nezávisle.[827] Za účelem ověřování zákonnosti zpracování údajů, provádění vlastní kontroly svých činností a zajišťování neporušenosti a bezpečnosti údajů vede Europol záznamy nebo dokumentace svých činností zpracování údajů. Tyto logy obsahují informace o činnostech zpracování v systémech automatizovaného zpracování týkajících se shromažďování, úpravy, konzultace, zveřejnění, kombinace a výmazu.[828]

Proti rozhodnutí EIOÚ je možné podat odvolání k SDEU.[829] Každý jednotlivec, který utrpěl škodu v důsledku protiprávního postupu zpracování údajů, má právo na náhradu škody buď od Europolu, nebo od příslušného členského státu, a to tím, že v prvním uvedeném případě podá žalobu u SDEU nebo v druhém uvedeném případě u příslušného vnitrostátního soudu.[830] Kromě toho může přezkoumávat činnosti Europolu specializovaná skupina pro společnou parlamentní kontrolu vnitrostátních parlamentů a Evropského parlamentu.[831] Každý jednotlivec má právo na přístup ke svým osobním údajům, které o něm může Europol mít, a dále právo požádat o ověření, opravu nebo výmaz těchto osobních údajů. U těchto práv mohou existovat výjimky a omezení.

824 Tamtéž, článek 43 a článek 44.

825 Tamtéž, článek 45.

826 Tamtéž, čl. 42 odst. 1.

827 Tamtéž, čl. 42 odst. 1.

828 Tamtéž, článek 40.

829 Tamtéž, článek 48.

830 Tamtéž, článek 50.

831 Tamtéž, článek 51.

Eurojust

Eurojust, který byl zřízen v roce 2002, je subjekt EU se sídlem v Haagu. Podporuje justiční spolupráci při vyšetřováních a stíháních souvisejících se závažnou trestnou činností, jež se týká alespoň dvou členských států.[832] Eurojust je způsobilý:

- podporovat a zdokonalovat koordinaci vyšetřování a stíhání mezi příslušnými orgány různých členských států,

- usnadňovat výkon žádostí a rozhodnutí v souvislosti s justiční spoluprací.

Funkce Eurojustu plní národní členové. Každý členský stát jmenuje do Eurojustu jednoho soudce nebo státního zástupce, jehož status se řídí vnitrostátním právem a kterému jsou svěřeny nezbytné pravomoci k plnění úkolů nezbytných k podpoře a zdokonalení soudní spolupráce. Kromě toho jednají národní členové společně jako kolegium při plnění zvláštních úkolů Eurojustu.

Eurojust může zpracovávat osobní údaje, pokud je to nezbytné k dosažení jeho cílů. Tyto údaje jsou však omezeny na konkrétní informace o osobách podezřelých ze spáchání trestného činu nebo z účasti na takovém trestném činu nebo o osobách, které byly za tento trestný čin, který spadá do působnosti Eurojustu, odsouzeny. Eurojust rovněž smí zpracovávat některé informace týkající se svědků nebo obětí trestných činů spadající do oblasti působnosti Eurojustu.[833] Ve výjimečných případech Eurojust smí po omezenou dobu zpracovávat rozsáhlejší osobní údaje týkající se okolností trestného činu, pokud jsou bezprostředně důležité pro probíhající vyšetřování. V rámci svých pravomocí může Eurojust spolupracovat s dalšími orgány, institucemi a jinými subjekty EU a vyměňovat si s nimi osobní údaje. Eurojust rovněž může spolupracovat se třetími zeměmi a organizacemi a vyměňovat si s nimi osobní údaje.

832 Rada Evropské unie (2002), Rozhodnutí Rady 2002/187/SVV ze dne 28. února 2002 o zřízení Evropské jednotky pro soudní spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti, Úř. věst. 2002 L 63; Rada Evropské unie (2003), Rozhodnutí Rady 2003/659/SVV ze dne 18. června 2003, kterým se mění rozhodnutí 2002/187/SVV o zřízení Evropské jednotky pro soudní spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti, Úř. věst. 2003 L 44; Rada Evropské unie (2009), Rozhodnutí Rady 2009/426/SVV ze dne 16. prosince 2008 o posílení Eurojustu a o změně rozhodnutí 2002/187/SVV o zřízení Evropské jednotky pro soudní spolupráci (Eurojust) za účelem posílení boje proti závažné trestné činnosti, Úř. věst. 2009 L 138 (rozhodnutí o Eurojustu).

833 Konsolidované znění rozhodnutí Rady 2002/187/SVV ve znění rozhodnutí Rady 2003/659/SVV a rozhodnutí Rady 2009/426/SVV, čl. 15 odst. 2.

V souvislosti s ochranou údajů musí Eurojust zaručit úroveň ochrany, která přinejmenším odpovídá zásadám Modernizované úmluvy č. 108 a jejím následným změnám. V případech výměny údajů musí být dodržena zvláštní pravidla a omezení, která byla zavedena v dohodě o spolupráci nebo v pracovních ujednáních v souladu s rozhodnutími o Eurojustu a pravidly Eurojustu pro ochranu údajů.[834]

V Eurojustu byl ustaven nezávislý společný kontrolní orgán pověřený úkolem dohlížet na zpracování osobních údajů prováděné Eurojustem. Jednotlivci se mohou odvolat ke společnému kontrolnímu orgánu, pokud nejsou spokojeni s rozhodnutím Eurojustu ve věci žádosti o přístup, opravu, blokování nebo výmaz osobních údajů. Pokud Eurojust zpracovává osobní údaje protiprávně, odpovídá v souladu s vnitrostátním právem členského státu, kde se nachází jeho ústředí, tj. Nizozemska, za veškerou škodu způsobenou subjektu údajů.

Budoucnost

Evropská komise představila v červenci 2013 návrh nařízení za účelem reformy Eurojustu. Tento návrh byl doplněn o návrh na zřízení Úřadu evropského veřejného žalobce (viz níže). Cílem tohoto nařízení je zefektivnit funkce a strukturu tak, aby byly v souladu s Lisabonskou smlouvou. Kromě toho je cílem reformy dosáhnout jasného oddělení operativních úkolů Eurojustu, které provádí kolegium Eurojustu, od jeho administrativních úkolů. Díky tomu se budou moci členské státy také více soustředit na operativní úkoly. Bude zřízena nová výkonná rada, která bude mít za úkol pomáhat kolegiu při plnění administrativních úkolů.[835]

Úřad evropského veřejného žalobce

Členské státy mají výlučnou pravomoc v oblasti stíhání trestných činů podvodu a nesprávného nakládání s rozpočtovými prostředky EU, které mají také možné přeshraniční důsledky. Význam vyšetřování, stíhání a předvádění pachatelů těchto trestných činů před soud vzrostl, a to zejména kvůli přetrvávající hospodářské krizi.[836] Evropská komise navrhla nařízení o zřízení nezávislého Úřadu evropského

834 Ustanovení vnitřních pravidel Eurojustu pro zpracování a ochranu osobních údajů, Úř. věst. 2005 C 68/01, 19. března 2005, s. 1.

835 Viz webové stránky Evropské komise týkající se Eurojustu.

836 Viz Evropská komise (2013), Návrh nařízení Rady o zřízení Úřadu evropského veřejného žalobce, COM(2013) 534 final, Brusel, 17. července 2013, s. 1, a webové stránky Komise o úřadu EPPO.

veřejného žalobce (EPPO)[837] s cílem bojovat proti trestným činům poškozujícím nebo ohrožujícím finanční zájmy EU. Úřad EPPO bude zřízen prostřednictvím postupu posílené spolupráce, který umožňuje nejméně devíti členským státům navázat posílenou spolupráci v oblasti v rámci struktur EU, do které nejsou zapojeny ostatní země EU.[838] K posílené spolupráci se připojily Belgie, Bulharsko, Česká republika, Estonsko, Finsko, Francie, Chorvatsko, Kypr, Litva, Lotyšsko, Lucembursko, Německo, Portugalsko, Rumunsko, Řecko, Slovensko, Slovinsko a Španělsko a Itálie a Rakousko vyjádřily záměr se připojit.[839]

Úřad EPPO bude mít pravomoc vyšetřovat a stíhat podvody proti EU a jiné trestné činy poškozující nebo ohrožující finanční zájmy EU s cílem účinně koordinovat vyšetřování a stíhání v rámci odlišných vnitrostátních právních řádů a zlepšit využívání zdrojů a výměnu informací na evropské úrovni.[840]

Úřadu EPPO bude předsedat evropský veřejný žalobce a v každém členském státě se bude nacházet jeden evropský pověřený žalobce, který bude odpovědný za vedení vyšetřování a stíhání v daném členském státě.

Návrh stanoví silné záruky na zaručení práv osob, jichž se týkají stíhání úřadu EPPO, jak stanoví vnitrostátní právo, právo EU a Listina základních práv EU. Opatření v rámci vyšetřování, která se nejvíce dotýkají základních práv, budou vyžadovat předchozí oprávnění od vnitrostátního soudu.[841] Vyšetřování úřadu EPPO bude podléhat soudnímu přezkumu ze strany vnitrostátních soudů.[842]

Na zpracování administrativních osobních údajů, které bude provádět úřad EPPO, se použije nařízení o ochraně údajů orgány EU.[843] Pro zpracování osobních údajů

837 Evropská komise (2013), Návrh nařízení Rady o zřízení Úřadu evropského veřejného žalobce, COM(2013) 534 final, Brusel, 17. července 2013.

838 Smlouva o fungování EU, čl. 86 odst. 1 a čl. 329 odst. 1.

839 Viz Rada Evropské unie (2017), „*20 členských států se dohodlo na podrobnostech ohledně zřízení Úřadu evropského veřejného žalobce*“, tisková zpráva, 8. června 2017.

840 Evropská komise (2013), Návrh nařízení Rady o zřízení Úřadu evropského veřejného žalobce, COM(2013) 534 final, Brusel, 17. července 2013, s. 1 a s. 51–51. Viz webové stránky Komise týkající se úřadu EPPO.

841 Evropská komise (2013), Návrh nařízení Rady o zřízení Úřadu evropského veřejného žalobce, COM(2013) 534 final, Brusel, 17. července 2013, čl. 26 odst. 4.

842 Tamtéž, článek 36.

843 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

souvisejících s operativními záležitostmi bude mít úřad EPPO podobně jako Europol samostatný režim ochrany údajů, který bude podobný režimu, který v současnosti upravuje činnosti Europolu a Eurojustu, jelikož výkon pravomocí úřadu EPPO bude zahrnovat zpracovávání osobních údajů spolu s donucovacími a stíhajícími orgány na úrovni členského státu. Pravidla úřadu EPPO na ochranu údajů jsou proto téměř identická s pravidly uvedenými ve směrnici o ochraně údajů policií a trestním soudnictvím. Podle návrhu na zřízení úřadu EPPO musí být zpracování osobních údajů v souladu se zásadami zákonnosti a spravedlnosti, účelového omezení, minimalizace údajů, přesnosti, neporušenosti a důvěrnosti. Úřad EPPO musí v rozsahu, v jakém to bude možné, jasně rozlišovat mezi osobními údaji různých druhů subjektů údajů, jako jsou osoby odsouzené za trestný čin, osoby, které jsou pouze podezřelými, oběti a svědci. Musí rovněž usilovat o ověřování kvality zpracovávaných osobních údajů a rozlišovat, nakolik to bude možné, mezi osobními údaji založenými na faktech a osobními údaji založenými na osobních hodnoceních.

Návrh obsahuje ustanovení o právech subjektů údajů, zejména o právu na informace, právu na přístup k jejich osobním údajům, právu na ochranu, právu na výmaz a právu na omezení zpracování, a stanoví, že tato práva mohou být také vykonávána nepřímo prostřednictvím EIOÚ. Ztělesňuje rovněž zásadu bezpečnosti zpracování a zásadu odpovědnosti, protože ukládá úřadu EPPO, aby zavedl vhodná technická a organizační opatření k zajištění úrovně zabezpečení, která je vhodná vzhledem k rizikům, která zpracování představuje, aby uchovával záznamy o všech činnostech zpracování a aby prováděl před zahájením zpracování posouzení vlivu na ochranu osobních údajů, pokud druh zpracování (například zpracování zahrnující používání nových technologií) pravděpodobně povede k vysokému riziku pro práva jednotlivců. V neposlední řadě návrh stanoví, že kolegium jmenuje pověřence pro ochranu osobních údajů, který musí být řádně zapojen do všech záležitostí týkajících se ochrany osobních údajů a musí zajišťovat, aby úřad EPPO jednal v souladu s platnými právními předpisy v oblasti ochrany údajů.

8.3.2. Ochrana údajů v rámci společných informačních systémů na úrovni EU

Vedle výměny údajů mezi členskými státy a vytvoření specializovaných orgánů EU pro boj proti přeshraniční trestné činnosti, jako jsou Europol, Eurojust a úřad EPPO, bylo na úrovni EU vytvořeno několik společných informačních systémů s cílem umožnit a usnadnit spolupráci a výměnu údajů mezi příslušnými vnitrostátními orgány a orgány EU za konkrétními účely v oblasti ochrany hranic, imigrace a azylu

a cel. Jelikož schengenský prostor byl původně vytvořen prostřednictvím mezinárodní dohody nezávislé na právu EU, Schengenský informační systém (SIS) se vyvinul na základě multilaterálních dohod, které byly následně přeneseny do práva EU. Vízový informační systém (VIS), Eurodac, EUROSUR a Celní informační systém (CIS) byly vytvořeny jako nástroje řídící se právem EU.

O dohled nad těmito systémy se dělí vnitrostátní dozorové úřady a EIOÚ. K zajištění vysoké úrovně ochrany tyto úřady spolupracují v rámci skupin pro koordinaci dohledu, které se zabývají těmito rozsáhlými informačními systémy: 1) Eurodac, 2) Vízový informační systém, 3) Schengenský informační systém, 4) Celní informační systém a 5) Systém pro výměnu informací o vnitřním trhu.[844] Skupiny pro koordinaci dohledu se scházejí dvakrát ročně, předsedá jim zvolený předseda a přijímají pokyny, projednávají přeshraniční případy nebo přijímají jednotné rámce pro inspekce.

Za provozní řízení Schengenského informačního systému druhé generace (SIS II), Vízového informačního systému (VIS) a systému Eurodac odpovídá Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA)[845], zřízená v roce 2012. Hlavním úkolem agentury eu-LISA je zajistit účinný, bezpečný a nepřetržitý provoz informačních systémů. Je také zodpovědná za přijetí nezbytných opatření k zajištění zabezpečení systémů a údajů.

Schengenský informační systém

V roce 1985 uzavřelo několik členských států někdejšího Evropského společenství Dohodu mezi vládami států Hospodářské unie Beneluxu, Německa a Francie o postupném odstraňování kontrol na společných hranicích (Schengenskou dohodu), která měla za cíl vytvořit prostor volného pohybu osob, kterému nebrání hraniční kontroly uvnitř schengenského území.[846] Aby se vyvážilo ohrožení veřejné bezpečnosti, které by mohlo být důsledkem otevřených hranic, byly zavedeny posílené pohraniční kontroly na vnějších hranicích schengenského prostoru, jakož i úzká spolupráce mezi vnitrostátními policejními a justičními orgány.

844 Viz webovou stránku evropského inspektora ochrany údajů týkající se koordinace dohledu.

845 Nařízení Evropského parlamentu a Rady (EU) 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva, Úř. věst. 2011 L 286.

846 Dohoda mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích, Úř. věst. 2000 L 239.

Kvůli přistoupení dalších států k Schengenské dohodě byl schengenský systém nakonec začleněn do právního rámce EU Amsterodamskou smlouvou.[847] Provádění tohoto rozhodnutí započalo v roce 1999. Nejnovější verze Schengenského informačního systému, takzvaný SIS II, zahájila provoz 9. dubna 2013. Slouží nyní většině členských států EU,[848] dále Islandu, Lichtenštejnsku, Norsku a Švýcarsku.[849] K systému SIS II mají rovněž přístup Europol a Eurojust.

Systém SIS II tvoří centrální systém (C-SIS), vnitrostátní systém (N-SIS) v každém členském státě a komunikační infrastruktura mezi centrálním systémem a vnitrostátními systémy. C-SIS obsahuje některé údaje o osobách a předmětech vložené členskými státy. Systém SIS používají vnitrostátní orgány ostrahy hranic, policie, celní správa, orgány vydávající víza a justiční orgány v celém schengenském prostoru. Každý členský stát provozuje vnitrostátní kopii systému C-SIS, označovanou jako vnitrostátní schengenské informační systémy (N-SIS), které se nepřetržitě aktualizují, a tím aktualizují systém C-SIS. V systému SIS existují různé druhy záznamů:

- osoba nemá právo vstoupit nebo pobývat na schengenském území nebo
- osoba nebo předmět jsou hledány justičními nebo donucovacími orgány (např. evropský zatýkací rozkaz, žádosti o skryté kontroly) nebo
- osoba byla nahlášena jako pohřešovaná nebo
- předměty, například bankovky, vozidla, dodávky, palné zbraně a doklady totožnosti, byly nahlášeny jako odcizené nebo ztracené.

Pokud vznikne nový záznam, je třeba zahájit návazné činnosti prostřednictvím center SIRENE. Systém SIS II má nové funkce, jako je možnost zadat: biometrické údaje, jako jsou otisky prstů a fotografie, nebo nové kategorie záznamů, jako jsou odcizené čluny, letadla, kontejnery nebo platební prostředky, vylepšené záznamy o osobách a předmětech a kopie evropských zatýkacích rozkazů vztahujících se na osoby hledané za účelem zatčení, předání nebo vydání.

847 Evropská společenství (1997), Amsterodamská smlouva pozměňující Smlouvu o Evropské unii, smlouvy o založení Evropských společenství a některé související akty, Úř. věst. 1997 C 340.

848 Chorvatsko, Irsko a Kypr provádějí přípravné činnosti k začlenění do SIS II, ale dosud nejsou jeho součástí. Viz informace o Schengenském informačním systému, které jsou k dispozici na webových stránkách Generální ředitelství pro migraci a vnitřní věci Evropské komise.

849 Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosince 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II), Úř. věst. 2006 L 381, a Rada Evropské unie, rozhodnutí Rady 2007/533/SVV ze dne 12. června 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II), Úř. věst. 2007 L 205.

Systém SIS II je založen na dvou aktech, které se vzájemně doplňují: rozhodnutí o systému SIS II[850] a nařízení o systému SIS II[851]. Normotvůrce EU použil pro přijetí rozhodnutí a nařízení odlišný právní základ. Rozhodnutí upravuje používání systému SIS II pro účely v rámci policejní a soudní spolupráce v trestních záležitostech (dříve třetí pilíř EU). Nařízení se použije na postup týkající se záznamů spadajících do oblasti azylové, přistěhovalecké a jiných politik souvisejících s volným pohybem osob (dříve první pilíř). Postupy týkající se záznamů pro každý pilíř musely být upraveny samostatnými akty, jelikož oba právní akty byly přijaty před vstupem Lisabonské smlouvy v platnost a před zrušením struktury pilířů.

Oba právní akty obsahují pravidly o ochraně údajů. Rozhodnutí o systému SIS II zakazuje zpracovávání citlivých údajů.[852] Zpracování osobních údajů bude zahrnuto do působnosti Modernizované úmluvy č. 108.[853] Kromě toho mají osoby právo na přístup k osobním údajům, které se jich týkají a které jsou vloženy do systému SIS II.[854]

Nařízení o systému SIS II upravuje podmínky a postupy pro vkládání a zpracování záznamů týkajících se zamítnutí vstupu nebo pobytu občanů zemí mimo EU. Rovněž stanoví pravidla pro výměnu doplňujících a dalších informací pro účely vstupu do některého členského státu nebo pobytu v něm.[855] Toto nařízení obsahuje také pravidla o ochraně údajů. Citlivé kategorie údajů ve smyslu čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů nesmějí být zpracovávány.[856] Nařízení o systému SIS II rovněž obsahuje určitá práva pro subjekty údajů, a sice:

- právo na přístup k osobním údajům týkajícím se daného subjektu údajů,[857]
- právo na opravu věcně nepřesných údajů,[858]

850 Rozhodnutí Rady č. 2007/533/SVV ze dne 12. červen 2007 o zřízení, provozování a využívání Schengenského informačního systému druhé generace (SIS II), Úř. věst. L 205, 7. srpna 2007.

851 Nařízení Evropského parlamentu a Rady (ES) č. 1987/2006 ze dne 20. prosinec 2006 o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II), Úř. věst. L 381, 28. prosince 2006.

852 Rozhodnutí o systému SIS II, článek 56; nařízení o systému SIS II, článek 40.

853 Rozhodnutí o systému SIS II, článek 57.

854 Rozhodnutí o systému SIS II, článek 58; nařízení o systému SIS II, článek 41.

855 Nařízení o systému SIS II, článek 2.

856 Tamtéž, článek 40.

857 Tamtéž, čl. 41 odst. 1.

858 Tamtéž, čl. 41 odst. 5.

- právo na výmaz protiprávně uchovávaných údajů[859] a

- právo být informován, pokud je o subjektu údajů vydán záznam. Tyto informace se poskytnou písemně, společně s kopií vnitrostátního rozhodnutí, na jehož základě byl záznam pořízen, nebo s odkazem na toto rozhodnutí.[860]

Právo být informován se neuplatní, pokud 1) osobní údaje nebyly získány od dotyčného subjektu údajů a poskytnutí informací se ukáže jako nemožné nebo by vyžadovalo nepřiměřené úsilí, 2) subjekt údajů již tuto informaci má nebo 3) pokud vnitrostátní právo umožňuje omezení mimo jiné za účelem zajištění národní bezpečnosti, obrany nebo pro předcházení trestným činům.[861]

Jak rozhodnutí, tak nařízení o systému SIS stanoví, že přístupová práva jednotlivců v souvislosti se systémem SIS II mohou být vykonávána v jakémkoliv členském státě a bude se v této věci postupovat v souladu s vnitrostátním právním řádem daného členského státu.[862]

Příklad: Ve věci *Dalea v. Francie*[863] bylo stěžovateli zamítnuto udělení víz k návštěvě Francie, protože francouzské orgány uvedly v Schengenském informačním systému, že by mu měl být odepřen vstup. Stěžovatel neúspěšně usiloval o přístup k těmto údajům, o jejich opravu a výmaz u francouzské Komise pro ochranu údajů a nakonec i u Státní rady. ESLP rozhodl, že nahlášení stěžovatele do Schengenského informačního systému bylo v souladu s právem a sledovalo legitimní cíl ochránit národní bezpečnost. Jelikož stěžovatel neprokázal, jaká faktická škoda mu vznikla v důsledku odepření vstupu do schengenského prostoru, a protože byla zavedena dostatečná opatření na jeho ochranu před svévolnými rozhodnutími, byl zásah do jeho práva na respektování soukromého života přiměřený. Stěžovatelova stížnost podle článku 8 byla tudíž prohlášena za nepřípustnou.

Na vnitrostátní systém N-SIS dohlíží v každém členském státě příslušný vnitrostátní orgán dozoru. Vnitrostátní orgány dozoru musí zajistit, aby byl alespoň jednou za

859 Tamtéž, čl. 41 odst. 5.

860 Tamtéž, čl. 42 odst. 1.

861 Tamtéž, čl. 42 odst. 2.

862 Nařízení o systému SIS II, čl. 41 odst. 1 a rozhodnutí o systému SIS II, článek 58.

863 Rozsudek ESLP ze dne 2. února 2010, *Dalea v. Francie*, č. 964/07.

čtyři rok proveden audit činností zpracování údajů v systému N.SIS.[864] Vnitrostátní orgány dozoru a EIOÚ spolupracují a zajišťují koordinovaný dohled nad systémy N-SIS a EIOÚ je pak odpovědný za dohled nad systém C-SIS. Pro zajištění transparentnosti se každé dva roky zasílá společná zpráva o činnostech Evropskému parlamentu, Radě a agentuře eu-LISA. Skupina pro koordinaci dohledu (Supervision Coordination Group, SCG) v rámci systému SIS II byla zřízena, aby zajišťovala koordinaci dohledu nad systémem SIS, a schází se nejvýše dvakrát ročně. Tuto skupinu tvoří EIOÚ a zástupci dozorových úřadů těch členských států, které zavedly systém SIS II, jakož i Islandu, Lichtenštejnska, Norska a Švýcarska, protože systém SIS se vztahuje i na ně, jelikož jsou také členy schengenského prostoru.[865] Kypr, Chorvatsko a Irsko se dosud do systému SIS II nezapojily, a proto se zasedání skupiny SCG účastní pouze jako pozorovatelé. V rámci skupiny SCG aktivně spolupracují EIOÚ a vnitrostátní orgány dozoru formou výměny informací, vzájemné pomoci při provádění auditů a inspekcí, přípravy harmonizovaných návrhů pro společná řešení možných problémů a při zvyšování povědomí o právech na ochranu údajů.[866] Skupina SVG pro systém SIS II rovněž přijímá pokyny, které pomáhají subjektům údajů. Příkladem mohou být pokyny, které pomáhají subjektům údajů při výkonu jejich práv na přístup.[867]

Budoucnost

V roce 2016 provedla Evropská komise hodnocení systému SIS[868], ze kterého vyplynulo, že byly zavedeny vnitrostátní mechanismy, které umožňují subjektům údajů přístup k jejich osobním údajům v systému SIS II, jejich opravu a výmaz a které umožňují získat odškodnění v souvislosti s nepřesnými údaji. Za účelem zlepšení účinnosti a účelnosti systému SIS II předložila Evropská komise tři návrhy nařízení:

- nařízení týkající se zřízení, provozu a využívání systému SIS v oblasti hraničních kontrol, kterým se zruší nařízení o systému SIS II,

---

864 Nařízení o systému SIS II, čl. 60 odst. 2.

865 Viz webovou stránku evropského inspektora ochrany údajů týkající se Schengenského informačního systému.

866 Nařízení o systému SIS II, článek 46 a rozhodnutí o systému SIS II, článek 62.

867 Viz SCG pro systém SIS II, *The Schengen Information System. A guide for exercising the right of access [Schengenský informační systém. Pokyny pro výkon práva na přístup]*, dostupné na webové stránce EIOÚ.

868 Evropská komise (2016), Zpráva Komise Evropskému parlamentu a Radě o hodnocení Schengenského informačního systému druhé generace (SIS II) v souladu s čl. 24 odst. 5, čl. 43 odst. 3 a čl. 50 odst. 5 nařízení (ES) č. 1987/2006 a čl. 59 odst. 3 a čl. 66 odst. 5 rozhodnutí 2007/533/SVV, COM(2016) 880 final, Brusel, 21. prosince 2016.

- nařízení týkající se zřízení, provozu a využívání systému SIS v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, kterým se zruší mimo jiné rozhodnutí o systému SIS II, a

- nařízení týkající se využívání systému SIS při navracení neoprávněně pobývajících státních příslušníků třetích zemí.

Je důležité připomenout, že návrhy umožňují zpracovávání dalších kategorií biometrických údajů – kromě fotografií a otisků prstů, které jsou již nyní součástí stávajícího režimu systému SIS II. V databázi SIS budou také ukládána zobrazení obličeje, otisky dlaně a profily DNA. Dále pak zatímco nařízení a rozhodnutí o systému SIS II stanovily možnost vyhledávání otisků prstů za účelem identifikace osoby, návrhy stanoví povinnost provést vyhledávání v případě, že totožnost osoby nelze určit jinými prostředky. Zobrazení tváře, fotografie a otisky dlaně budou použity k vyhledávání v systému a k identifikaci osob, jakmile toto vyhledávání bude technicky možné. Nová pravidla o biometrických prostředcích přiřazování představují mimořádné riziko pro práva jednotlivců. EIOÚ ve svém stanovisku k návrhům Komise[869] konstatoval, že biometrické údaje jsou velmi citlivé a jejich zavedení do takto rozsáhlé databáze by mělo vycházet z posouzení nutnosti jejich začlenění do systému SIS, které bude založeno na důkazech. Jinými slovy tedy řekl, že by měla být prokázána nezbytnost zpracovávání nových prostředků přiřazování. EIOÚ se rovněž domníval, že je třeba dále vyjasnit, jaký druh informací může být součástí profilu DNA. Jelikož profil DNA může obsahovat citlivé informace (nejzjevnějším příkladem by mohly být informace o zdravotních problémech), měly by profily DNA uložené v systému SIS obsahovat: „pouze minimum informací, které je naprosto nezbytné k identifikaci pohřešovaných osob, a bez informací výlučně o zdraví, rasovém původu a veškerých dalších citlivých informací".[870] Návrhy však stanoví dodatečné záruky s cílem omezit shromažďování a další zpracování údajů na míru nezbytně nutnou a z operativního hlediska potřebnou a omezit přístup k těmto údajům pouze na osoby, které mají operativní potřebu osobní údaje zpracovávat.[871] Návrhy rovněž zmocňují agenturu eu-LISA k vypracování zpráv o kvalitě údajů pro jednotlivé členské státy

869 EIOÚ (2017), EDPS Opinion on the new legal basis of the Schengen Information System [Stanovisko EIOÚ k novému právnímu základu Schengenského informačního systému], stanovisko 7/2017, 2. května 2017.

870 Tamtéž, bod 22.

871 Evropská komise (2016), Návrh nařízení Evropského parlamentu a Rady o zřízení, provozu a využívání Schengenského informačního systému (SIS) v oblasti policejní spolupráce a justiční spolupráce v trestních věcech, o změně nařízení (EU) č. 515/2014 a o zrušení nařízení (ES) č. 1986/2006, rozhodnutí Rady 2007/533/SVV a rozhodnutí Komise 2010/261/EU, COM(2016) 883 final, Brusel, 21. prosince 2016.

v pravidelných intervalech s cílem pravidelně přezkoumávat záznamy za účelem zajištění kvality údajů.[872]

Vízový informační systém

Vízový informační systém (VIS), který rovněž provozuje agentura eu-LISA, byl vyvinut, aby podporoval provádění společné vízové politiky EU.[873] Systém VIS umožňuje státům schengenského prostoru vyměňovat si údaje týkající se žadatelů o víza prostřednictvím plně centralizovaného systému, který propojuje konzuláty a velvyslanectví schengenských států nacházejících se v zemích mimo EU s hraničními přechody na vnějších hranicích všech schengenských zemí. Systém VIS zpracovává údaje o žádostech o krátkodobá víza za účelem návštěvy schengenského prostoru nebo tranzitu. Systém VIS umožňuje pohraničním orgánům ověřit s pomocí biometrických prostředků přiřazování, zejména otisků prstů, zda daná osoba předkládající víza je jejich oprávněným držitelem, a identifikovat osoby bez dokladů nebo s podvodnými doklady.

Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS) upravuje podmínky a postupy pro předávání osobních údajů týkajících se žádostí o krátkodobá víza. Dohlíží rovněž na rozhodnutí přijatá na základě žádostí, včetně rozhodnutí o prohlášení víza za neplatné od počátku nebo jeho zrušení anebo prodloužení jeho platnosti.[874] Nařízení o VIS se týká hlavně údajů o žadateli, jeho vízech, fotografií, otisků prstů, odkazů na předchozí žádosti a souboru žádosti osob, které žadatele doprovázejí, nebo údajů o osobách, které ho pozvaly.[875] Přístup do systému VIS za účelem vložení, úpravy nebo výmazu údajů je omezen výlučně na vízové orgány, zatímco přístup k prohlížení údajů je poskytnut vízovým orgánům

872 Tamtéž, s. 15.

873 Rada Evropské unie (2004), Rozhodnutí Rady 2004/512/ES ze dne 8. června 2004 o zřízení Vízového informačního systému (VIS), Úř. věst. 2004 L 213; Nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy, Úř. věst. 2008 L 218 (nařízení o VIS); Rada Evropské unie (2008), Rozhodnutí Rady 2008/633/SVV ze dne 23. června 2008 o konzultačním přístupu určených orgánů členských států a Europolu do Vízového informačního systému (VIS) pro účely prevence, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů, Úř. věst. 2008 L 218.

874 Nařízení o VIS, článek 1.

875 Článek 5 nařízení Evropského parlamentu a Rady (ES) č. 767/2008 ze dne 9. července 2008 o Vízovém informačním systému (VIS) a o výměně údajů o krátkodobých vízech mezi členskými státy (nařízení o VIS), Úř. věst. 2008 L 218.

a orgánům příslušným k provádění kontrol na vnějších hraničních přechodech, orgánům provádějícím imigrační kontrolu a azylovým orgánům.

Za určitých podmínek mohou příslušné vnitrostátní policejní orgány a Europol požádat o přístup k údajům vloženým do systému VIS za účelem prevence, odhalování či vyšetřování teroristických a jiných trestných činů.[876] Jelikož byl systém VIS navržen jako nástroj na podporu provádění společné vízové politiky, došlo by v případě, že by se ze systému VIS stal nástroj prosazování práva, k porušení zásady účelového omezení, která, jak je vysvětleno v oddíle 3.2, stanoví povinnost, aby osobní údaje byly zpracovávány pouze pro určité, výslovně vyjádřené a legitimní účely a byly přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány. Z tohoto důvodu není vnitrostátním donucovacím orgánům a Europolu udělen rutinní přístup k databázi VIS. Přístup může být udělen pouze v jednotlivých případech a musí být doplněn o přísné záruky. Podmínky a záruky pro přístup k systému VIS a jeho prohlížení ze strany těchto orgánů byly upraveny v rozhodnutí Rady 2008/633/SVV.[877]

Kromě toho stanoví nařízení o VIS práva subjektů údajů. Jsou jimi:

- Právo být informován odpovědným členským státem o totožnosti a kontaktních údajích správce údajů pověřeného zpracováváním osobních údajů v daném členském státě, účelech zpracovávání jejich osobních údajů v systému VIS, kategoriích osob, jimž mohou být údaje předány (příjemci) a o době uchovávání údajů. Kromě toho musí být žadatelé o víza informováni o skutečnosti, že shromažďování jejich osobních údajů v rámci systému VIS je povinné za účelem přezkumu jejich žádosti, zatímco členské státy je musí rovněž informovat o existenci jejich práva na přístup k údajům a práva na požádání o jejich opravu nebo výmaz a o postupech, které jim umožní tato práva vykonávat.[878]

- Právo na přístup k osobním údajům, které se jich týkají a které jsou vloženy do systému VIS.[879]

876 Rada Evropské unie (2008), Rozhodnutí Rady 2008/633/SVV ze dne 23. června 2008 o konzultačním přístupu určených orgánů členských států a Europolu do Vízového informačního systému (VIS) pro účely prevence, odhalování a vyšetřování teroristických trestných činů a jiných závažných trestných činů, Úř. věst. 2008 L 218.

877 Tamtéž.

878 Nařízení o VIS, článek 37.

879 Tamtéž, čl. 38 odst. 1.

- Právo na opravu nepřesných údajů.[880]
- Právo na výmaz protiprávně uchovávaných údajů.[881]

Za účelem zajištění dohledu nad systém VIS byla zřízena skupina SCG pro systém VIS. Tvoří ji zástupci EIOÚ a vnitrostátních orgánů dozoru, kteří se scházejí dvakrát ročně. Členy této skupiny jsou zástupci 28 členských států EU a Islandu, Lichtenštejnska, Norska a Švýcarska.

Eurodac

Eurodac je zkratka slov evropská daktyloskopie (european dactyloscopy)[882]. Jedná se o centralizovaný systém, který obsahuje otisky prvků státních příslušníků třetí země a osob bez státní příslušnosti, kteří žádají o azyl v jednom ze členských států EU.[883] Systém je v provozu od ledna 2003 v návaznosti na přijetí nařízení Rady č. 2725/2000. Přepracované znění nabylo účinnosti v roce 2015. Účelem systému je především pomáhat při určování, který členský stát by měl být příslušný k posouzení konkrétní žádosti o azyl podle nařízení (ES) č. 604/2013. Toto nařízení stanoví kritéria pro určení členského státu příslušného k posuzování žádosti o poskytnutí mezinárodní ochrany podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států (nařízení Dublin III).[884] Osobní údaje v systému Eurodac plní především účel usnadnit uplatňování nařízení Dublin III.[885]

880 Tamtéž, čl. 38 odst. 2.

881 Tamtéž, čl. 38 odst. 2.

882 Viz webovou stránku evropského inspektora ochrany údajů týkající se systému Eurodac.

883 Nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 2000 o zřízení systému Eurodac pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy, Úř. věst. 2000 L 316; nařízení Rady (ES) č. 407/2002 ze dne 28. února 2002, kterým se stanoví některá prováděcí pravidla k nařízení (ES) č. 2725/2000 o zřízení systému Eurodac pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy, Úř. věst. 2002 L 62 (nařízení o Eurodacu), nařízení Evropského parlamentu a Rady (EU) č. 603/2013 ze dne 26. června 2013 o zřízení systému „Eurodac" pro porovnávání otisků prstů za účelem účinného uplatňování nařízení (EU) č. 604/2013 kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států, a pro podávání žádostí orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva a o změně nařízení (EU) č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva, Úř. věst. 2013 L 180, s. 1 (přepracované nařízení o Eurodacu).

884 Nařízení Evropského parlamentu a Rady (EU) č. 604/2013 ze dne 26. června 2013, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států, Úř. věst. 2013 L 180 (nařízení Dublin III).

885 Přepracované nařízení o Eurodacu, Úř. věst. 2013 L 180, s. 1, čl. 1 odst. 1.

Vnitrostátní donucovací orgány a Europol smějí porovnávat otisky prstů spojené s vyšetřováním trestných činů s otisky prstů obsaženými v systému Eurodac, ale pouze pro účely prevence, odhalování a vyšetřování teroristických a jiných závažných trestných činů. Jelikož systém Eurodac byl koncipován jako nástroj na podporu provádění azylové politiky EU, a nikoliv jako nástroj prosazování práva, mají donucovací orgány přístup k databázi pouze ve zvláštních případech, za zvláštních okolností a při splnění přísných podmínek.[886] V případě dalšího použití údajů pro účely prosazování práva se použije směrnice o ochraně údajů policií a trestním soudnictvím, zatímco údaje použité především za účelem usnadnění provádění nařízení Dublin III jsou chráněny podle obecného nařízení o ochraně osobních údajů. Další předání osobních údajů získaných členským státem nebo Europolem podle přepracovaného nařízení o Eurodacu jakékoliv třetí zemi, mezinárodní organizaci či soukromému subjektu usazenému v EU nebo mimo EU je zakázáno.[887]

Systém Eurodac tvoří ústřední jednotka provozovaná agenturou eu-LISA, která slouží k ukládání a porovnávání otisků prstů, a systém pro elektronické předávání údajů mezi členskými státy a ústřední databází. Členské státy sejmou a předají otisky prstů každé osoby starší 14 let žádající o azyl na jejich území a každého státního příslušníka země mimo EU nebo osoby bez státní příslušnosti starší 14 let, která byla zadržena v souvislosti s neoprávněným překročením vnější hranice daného členského státu. Členské státy také mohou sejmout a předat otisky prstů státních příslušníků zemí mimo EU nebo osob bez státní příslušnosti, u nichž bylo zjištěno, že pobývají na území tohoto členského státu bez povolení.

Ačkoliv mohou všechny členské státy nahlížet do systému Eurodac a požádat o porovnání údajů o otiscích prstů, pouze ten členský stát, který otisky prstů shromáždil a předal ústřední jednotce, má právo údaje měnit, a to tím, že je opraví, doplní nebo vymaže.[888] Agentura eu-LISA uchovává záznamy o veškerém zpracování údajů za účelem sledování ochrany údajů a zajištění jejich bezpečnosti.[889] Vnitrostátní orgány dozoru pomáhají a radí subjektům údajů ohledně výkonu jejich práv.[890] Oprava a předání údajů o otiscích prstů podléhá soudnímu přezkumu vnit-

886 Tamtéž, čl. 1 odst. 2.
887 Tamtéž, článek 35.
888 Tamtéž, článek 27.
889 Tamtéž, článek 28.
890 Tamtéž, článek 29.

rostátními soudy.[891] Nařízení o ochraně údajů orgány EU[892] a dohled ze strany EIOÚ se týká činností zpracování ústředního systému, který s ohledem na systém Eurodac spravuje agentura eu-LISA.[893] Pokud daná osoba utrpí škodu v důsledku protiprávní operace zpracování nebo jakéhokoliv jiného jednání, které je neslučitelné s nařízením o Eurodacu, má tato osoba nárok na náhradu škody od členského státu, který je za tuto škodu zodpovědný.[894] Je však třeba zdůraznit, že žadatelé o azyl jsou zvlášť zranitelnou skupinou osob a často podnikli dlouhou a riskantní cestu. Kvůli své zranitelnosti a nejistému postavení, v němž se nachází, zatímco se přezkoumává jejich žádost o azyl, může se v praxi výkon jejich práv, včetně práva na náhradu, ukázat jako obtížný.

Aby mohly členské státy používat systém Eurodac pro účely prosazování práva, musejí určit orgány, které budou mít právo požádat o přístup, jakož i orgány, které budou ověřovat, zda jsou žádosti o porovnání zákonné.[895] Přístup vnitrostátních orgánů a Europolu k údajům o otiscích prstů v systému Eurodac se řídí velmi přísnými podmínkami. Dožadující orgán musí předložit odůvodněnou elektronickou žádost teprve poté, co provede porovnání údajů s jinými dostupnými informačními systémy, jako jsou vnitrostátní databáze otisků prstů a systém VIS. Musí existovat převažující zájem zachovat veřejnou bezpečnost, na základě kterého se porovnání stává přiměřeným. Porovnání musí být skutečně nezbytné, souviset s daným případem a musí existovat rozumné důvody pro domněnku, že porovnání významně přispěje k prevenci, odhalování nebo vyšetřování kteréhokoliv z dotčených trestných činů, zejména pokud existuje odůvodněné podezření, že podezřelý, pachatel nebo oběť teroristického trestného činu nebo jiného závažného trestného činu spadá do kategorie, u které se shromažďují otisky prstů v systému Eurodac. Porovnání je třeba provést výlučně s údaji o otiscích prstů. Europol musí také získávat povolení od členského státu, který údaje o otiscích prstů shromáždil.

Osobní údaje uložené v systému Eurodac, které se týkají žadatelů o azyl, se uchovávají po dobu 10 let ode dne, kdy byly otisky prstů sejmuty, ledaže subjekt údajů

891 Tamtéž, článek 29.

892 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

893 Přepracované nařízení o Eurodacu, Úř. věst. 2013 L 180, s. 1, článek 31.

894 Tamtéž, článek 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination" [Nové nařízení o EURODACu: otisky prstů jako zdroj neformální diskriminace], *Baltic Journal of European Studies Tallinn University of Technology*, sv. 5, č. 2, s. 108–129.

získá občanství některého členského státu EU. V takovém případě, musí být údaje neprodleně smazány. Údaje týkající se cizích státních příslušníků zadržených za neoprávněné překročení vnější hranice se uchovávají po dobu 18 měsíců. Tyto údaje musí být neprodleně vymazány, pokud subjekt údajů obdrží povolení k pobytu, opustí území EU nebo získá občanství některého členského státu. Údaje osob, kterým byl udělen azyl, jsou i nadále dostupné pro účely srovnávání v souvislosti s prevencí, odhalováním a vyšetřováním teroristických a jiných závažných trestných činů po dobu tří let.

Kromě všech členských států EU používají systém Eurodac na základě mezinárodních dohod i Island, Norsko, Lichtenštejnsko a Švýcarsko.

Za účelem dozoru nad systémem Eurodac byla zřízena skupina SCG. Tvoří ji zástupci EIOÚ a vnitrostátních orgánů dozoru, kteří se scházejí dvakrát ročně. Členy této skupiny jsou zástupci 28 členských států EU a Islandu, Lichtenštejnska, Norska a Švýcarska.[896]

Budoucnost

V květnu 2016 Komise vydala návrh nového přepracovaného znění nařízení o Eurodacu jako součást reformy, která má zlepšit fungování společného evropského azylového systému (CEAS).[897] Navrhované přepracované znění je důležité, protože významně rozšíří oblast působnosti původní databáze Eurodac. Tato databáze byla původně vytvořena za účelem provádění systému CEAS prostřednictvím poskytování důkazů v podobě otisků prstů s cílem umožnit určit, který členský stát je příslušný k přezkoumání žádosti o azyl předložené v EU. Navrhované přepracované znění rozšíří oblast působnosti databáze, aby usnadnila navracení nelegálních migrantů.[898] Vnitrostátní orgány budou schopny nahlédnout do databáze za účelem identifikace státních příslušníků třetích zemí, kteří pobývají v EU neoprávněně nebo kteří neoprávněně vstoupili do EU, s cílem získat důkazy, které pomohou členským státům s navracením těchto jednotlivců. Navíc zatímco právní režim, který platí

896 Viz webovou stránku evropského inspektora ochrany údajů týkající se systému Eurodac.

897 Návrh nařízení Evropského parlamentu a Rady o zřízení systému Eurodac pro porovnávání otisků prstů za účelem účinného uplatňování [nařízení (ES) č. 604/2013, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států], za účelem identifikace neoprávněně pobývajícího státního příslušníka třetí země nebo osoby bez státní příslušnosti a o žádostech orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva (přepracované znění), COM(2016) 272 final, 4. května 2016.

898 Viz důvodovou zprávu návrhu, s. 3.

v současnosti, ukládá pouze shromažďování a ukládání otisků prstů, návrh zavádí shromažďování zobrazení obličeje jednotlivců[899], což je další druh biometrických údajů. Návrh má také snížit minimální věk dětí, jimž lze snímat biometrické údaje – na šest let[900] namísto 14 let, což je minimální věk podle nařízení z roku 2013. Rozšířená oblast působnosti návrhu znamená, že bude představovat zásah do práv na ochranu soukromí a údajů více jednotlivců, kteří mohou být zařazeni do databáze. Aby byl tento zásah vyvážen, usiluje návrh a pozměňovací návrhy předložené výborem LIBE Evropského parlamentu[901] o posílení povinností v oblasti ochrany údajů. V době psaní této příručky stále probíhaly diskuse o návrhu v Parlamentu a Radě.

Eurosur

Evropský systém ostrahy hranic (Eurosur)[902] je navržen tak, aby posílil ochranu vnějších schengenských hranic prostřednictvím odhalování, prevence a boje proti nelegální imigraci a přeshraniční trestné činnosti. Zlepšuje výměnu informací a operativní spolupráci mezi vnitrostátními koordinačními centry a agenturou Frontex, což je agentura EU pověřená vývojem a prováděním nové koncepce integrované správy hranic.[903] Níže jsou uvedeny obecné cíle systému:

899 Návrh nařízení Evropského parlamentu a Rady o zřízení systému Eurodac pro porovnávání otisků prstů za účelem účinného uplatňování [nařízení (ES) č. 604/2013, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států], za účelem identifikace neoprávněně pobývajícího státního příslušníka třetí země nebo osoby bez státní příslušnosti a o žádostech orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva (přepracované znění), COM(2016) 272 final, 4. května 2016, čl. 2 odst. 1.

900 Tamtéž, čl. 2 odst. 2.

901 Evropský parlament, *Zpráva o návrhu nařízení Evropského parlamentu a Rady o zřízení systému Eurodac pro porovnávání otisků prstů za účelem účinného uplatňování [nařízení (ES) č. 604/2013, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o mezinárodní ochranu podané státním příslušníkem třetí země nebo osobou bez státní příslušnosti v některém z členských států], za účelem identifikace neoprávněně pobývajícího státního příslušníka třetí země nebo osoby bez státní příslušnosti a o žádostech orgánů pro vymáhání práva členských států a Europolu o porovnání údajů s údaji systému Eurodac pro účely vymáhání práva (přepracované znění)*, PE 597.620v03-00, 9. června 2017.

902 Nařízení Evropského parlamentu a Rady (EU) č. 1052/2013 ze dne 22. října 2013, kterým se zřizuje Evropský systém ostrahy hranic (EUROSUR), Úř. věst. 2013 L 295.

903 Nařízení Evropského parlamentu a Rady (EU) 2016/1624 ze dne 14. září 2016 o Evropské pohraniční a pobřežní stráži a o změně nařízení Evropského parlamentu a Rady (EU) 2016/399 a zrušení nařízení Evropského parlamentu a Rady (ES) č. 863/2007, nařízení Rady (ES) č. 2007/2004 a rozhodnutí Rady 2005/267/ES, Úř. věst. L 251.

- snížit počet nezákonných přistěhovalců, kterým se podaří vstoupit do EU, aniž by byli odhaleni,

- snížit počet úmrtí nelegálních migrantů tím, že se podaří zachránit více životů na moři,

- posílit vnitřní bezpečnost EU jako celku tím, že se přispěje k předcházení přeshraniční trestné činnosti.[904]

Systém Eurosur zahájil činnost dne 2. prosince 2013 ve všech členských státech s vnějšími hranicemi a dne 1. prosince 2014 ve všech ostatních. Nařízení se použije na ostrahu vnější pozemní, námořní a vzdušné hranice členských států. Systém Eurosur vyměňuje a zpracovává informace ve velmi omezené míře, protože členské státy a agentura Frontex jsou oprávněny pouze k výměně registračních čísel lodí. Systém Eurosur vyměňuje operativní informace, jako je lokace hlídek a incidentů, a vyměněné informace zpravidla nemohou obsahovat osobní údaje.[905] Ve výjimečných případech, pokud se osobní údaje vyměňují v rámci systému Eurosur, stanoví nařízení, že se v plném rozsahu uplatní obecný právní rámec EU týkající se ochrany údajů.[906]

Systém Eurosur tudíž zajišťuje právo na ochranu údajů, konkrétně tím, že uvádí, že výměny osobních údajů musejí být v souladu s kritérii a zárukami stanovenými směrnicí o ochraně údajů policií a trestním soudnictvím a obecným nařízením o ochraně osobních údajů.[907]

904 Viz též: Evropská komise (2008), *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Prozkoumání vytvoření Evropského systému kontroly hranic (EUROSUR)*, COM(2008) 68 final, Brusel, 13. února 2008; Evropská komise (2011), *Posouzení dopadu k návrhu nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropský systém ostrahy hranic (EUROSUR)*, pracovní dokument útvarů Komise, SEC(2011) 1536 final, Brusel,12. prosince 2011, s. 18.

905 Evropská komise, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell* [EUROSUR: Ochrana vnější schengenské hranice – ochrana života migrantů. Systém EUROSUR ve zkratce], 29. listopadu 2013.

906 Nařízení 1052/2013, 13. bod odůvodnění a článek 13.

907 Tamtéž, 13. bod odůvodnění a článek 13.

Celní informační systém

Dalším důležitým informačním systémem zřízeným na úrovni EU je celní informační systém (CIS).[908] V průběhu vytváření vnitřního trhu byly zrušeny všechny kontroly a formality týkající se přesunu zboží na území EU, což vedlo k vyššímu riziku podvodů. Toto riziko bylo vyváženo intenzivnější spoluprací mezi celními orgány členských států. Účelem systému CIS je pomoci členským státům zabránit různým případům porušení vnitrostátních právních předpisů a předpisů EU v oblasti cel a zemědělství, tyto případy vyšetřovat a stíhat. Systém CIS je zřízen dvěma právními akty přijatými na odlišných právních základech: nařízení Rady (ES) č. 515/97 se týká spolupráce mezi jednotlivými vnitrostátními správními orgány za účelem boje proti podvodům v souvislosti s celní unií a společnou zemědělskou politikou, zatímco rozhodnutí Rady 2009/917/SVV má za cíl pomoci zabránit vážným případům porušení celních právních předpisů, tyto případy vyšetřovat a stíhat. To znamená, že systém CIS se nezabývá pouze prosazováním práva.

K informacím obsaženým v systému CIS patří osobní údaje týkající se komodit, dopravních prostředků, podniků, osob, zboží a zajištěné, zabrané nebo propadlé hotovosti. Kategorie údajů, které je možné zpracovávat, jsou jasně definovány, a patří k nim jména, státní příslušnost, pohlaví, místo a datum narození dotčených jednotlivců, důvod pro začlenění jejich údajů do systému a registrační značka dopravních prostředků.[909] Tyto informace mohou být použity výlučně pro účely pozorování, zpravodajství a provádění zvláštních inspekcí nebo pro účely strategické a operativní analýzy týkající se osob podezřelých z porušení ustanovení celních předpisů.

Přístup k systému CIS se poskytuje vnitrostátním celním, daňovým, zemědělským, zdravotnickým a policejním orgánům, ale také Europolu a Eurojustu.

Zpracování osobních údajů musí být prováděno v souladu se zvláštními pravidly stanovenými v nařízení č. 515/97 a rozhodnutí Rady 2009/917/SVV, jakož i v souladu s ustanoveními obecného nařízení o ochraně osobních údajů, nařízení o ochraně údajů orgány EU, Modernizovanou úmluvou č. 108 a doporučením o policii. EIOÚ

908 Rada Evropské unie (1995), Akt Rady ze dne 26. července 1995 o vypracování Úmluvy o používání informační technologie pro celní účely, Úř. věst. 1995 C 316, ve znění: Rada Evropské unie (2009), Nařízení č. 515/97 ze dne 13. března 1997 o vzájemné pomoci mezi správními orgány členských států a jejich spolupráci s Komisí k zajištění řádného používání celních a zemědělských předpisů, Rozhodnutí Rady 2009/917/SVV ze dne 30. listopadu 2009 o používání informačních technologií pro celní účely, Úř. věst. 2009 L 323 (rozhodnutí o systému CIS).

909 Viz rozhodnutí o systému CIS, článek 24, 25 a 28.

je odpovědný za dohled nad tím, aby systém CIS byl v souladu s nařízením (ES) č. 45/2001. Nejméně jednou ročně svolává schůzi se všemi vnitrostátními dozorovými úřady v oblasti ochrany údajů, které jsou příslušné k dozorovým otázkám spojeným se systémem SIS.

Interoperabilita mezi informačními systémy EU

Řízení migrace, integrovaná správa vnějších hranic EU a boj proti terorismu a přeshraniční trestné činnosti představují důležité výzvy a v globalizovaném světě jsou stále složitější. V uplynulých letech pracovala EU na novém, komplexním přístupu k zaručení a zachování bezpečnosti, aniž by byly narušeny hodnoty EU a základní svobody. Při tomto úsilí má klíčový význam účinná výměna informací mezi vnitrostátními orgány prosazování práva a mezi členskými státy a příslušnými agenturami EU.[910] Stávající informační systémy EU pro správu hranic a vnitřní bezpečnosti mají každý svůj vlastní cíl, institucionální uspořádání, subjekty údajů a uživatele. EU pracuje na nápravě nedostatků, pokud jde o funkčnost roztříštěné správy údajů v EU mezi jednotlivými informačními systémy, jako jsou SIS II, VIS a Eurodac, a zkoumá potenciál pro interoperabilitu.[911] Hlavním cílem je zajistit, aby příslušné policejní, celní a soudní orgány systematicky měly informace nezbytné k plnění svých úkolů a současně byla zachována rovnováha s ohledem na právo na soukromí, právo na ochranu údajů a další základní práva.

Interoperabilita je „schopnost informačních systémů provádět výměnu údajů a umožňovat sdílení informací".[912] Tato výměna nesmí být v rozporu s nezbytně

910 Evropská komise (2016), Sdělení Komise Evropskému parlamentu a Radě: Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final, Brusel, 6. dubna 2016, Evropská komise (2016), sdělení Komise Evropskému parlamentu, Evropské Radě a Radě: Posilování bezpečnosti ve světě mobility: Zdokonalování výměny informací v boji proti terorismu a pevnější vnější hranice, COM(2016) 602 final, Brusel, 14. září 2016, Evropská komise (2016), Návrh nařízení Evropského parlamentu a Rady o využívání Schengenského informačního systému při navracení neoprávněně pobývajících státních příslušníků třetích zemí. Viz také sdělení Komise Evropskému parlamentu, Evropské radě a Radě: Sedmá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii, COM(2017) 261 final, Brusel, 16. května 2017.

911 Rada Evropské unie (2005), Haagský program: posílení svobody, bezpečnosti a práva v Evropské unii, Úř. věst. 2005 C 53, Evropská komise (2010), Sdělení Komise Evropskému parlamentu a Radě: Přehled o správě informací v prostoru svobody, bezpečnosti a práva, COM(2010) 385 final, Evropská komise (2016), Sdělení Komise Evropskému parlamentu a Radě: Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final, Brusel, 6. dubna 2016, Evropská komise (2016), Rozhodnutí Komise ze dne 17. června 2016 o zřízení expertní skupiny na vysoké úrovni pro informační systémy a interoperabilitu, Úř. věst. 2016 C 257.

912 Evropská komise (2016), Sdělení Komise Evropskému parlamentu a Radě: Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final, 6. dubna 2016, s. 14.

přísnými pravidly týkajícími se přístupu a užívání, jež zaručuje obecné nařízení o ochraně osobních údajů, směrnice o ochraně údajů policií a trestním soudnictvím, Listina základních práv EU a veškeré další příslušné předpisy. Jakékoliv integrované řešení v oblasti řízení údajů nesmí mít nepříznivý vliv na zásadu účelového omezení a záměrnou a standardní ochranu údajů.[913]

Kromě zlepšení funkcí tří hlavních informačních systémů – SIS II, VIS a Eurodac – navrhla Komise zřídit čtvrtý centralizovaný systém správy hranic, který by se zabýval státními příslušníky třetích zemí: systém vstupu/výstupu (EES)[914], jehož zavedení se očekává do roku 2020.[915] Komise rovněž vydala návrh na řízení Evropského systému pro cestovní informace a povolení (ETIAS)[916], což je systém, který bude shromažďovat informace o osobách cestujících do EU v rámci bezvízového styků s cílem umožnit vyspělé kontroly nelegální migrace a bezpečnostní kontroly.

913 Tamtéž, s. 4–5.

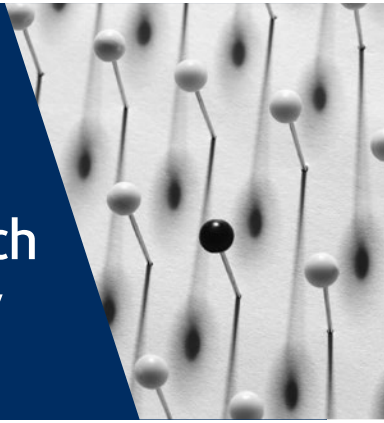
914 Evropská komise (2016), Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje systém vstupu/výstupu (EES) pro registraci údajů o vstupu a výstupu a údajů o odepření vstupu, pokud jde o státní příslušníky třetích zemí překračující vnější hranice členských států Evropské unie, kterým se stanoví podmínky přístupu do systému EES pro účely vymáhání práva a kterým se mění nařízení (ES) č. 767/2008 a nařízení (EU) č. 1077/2011, COM(2016) 194 final, Brusel, 6. dubna 2016.

915 Evropská komise (2016), Sdělení Komise Evropskému parlamentu a Radě: Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost, COM(2016) 205 final, 6. dubna 2016, s. 5.

916 Evropská komise (2016), Návrh nařízení Evropského parlamentu a Rady, kterým se zřizuje evropský systém pro cestovní informace a povolení (ETIAS) a kterým se mění nařízení (EU) č. 515/2014, (EU) 2016/399, (EU) 2016/794 a (EU) 2016/1624, COM(2016) 731 final, 16. listopadu 2016.

9

Zvláštní druhy údajů a jejich příslušná pravidla ochrany údajů



EU	Pojednávaná témata	RE
Obecné nařízení o ochraně osobních údajů Směrnice o soukromí a elektronických komunikacích	**Elektronická komunikace**	Modernizovaná úmluva č. 108 Doporučení o telekomunikačních službách
Obecné nařízení o ochraně osobních údajů, článek 88	**Zaměstnanecký poměr**	Modernizovaná úmluva č. 108 Doporučení o zaměstnání Rozsudek ESLP z roku 2007, *Copland v. Spojené království*, č. 62617/00
Obecné nařízení o ochraně osobních údajů, čl. 9 odst. 2 písm. h) a i)	**Lékařské údaje**	Modernizovaná úmluva č. 108 Doporučení o zdravotních údajích Rozsudek ESLP z roku 1997, *Z v. Finsko*, č. 22009/93
Nařízení o klinických hodnoceních	**Klinická hodnocení**	
Obecné nařízení o ochraně osobních údajů, čl. 6 odst. 4, článek 89	**Statistika**	Modernizovaná úmluva č. 108 Doporučení o statistických údajích

EU	Pojednávaná témata	RE
Nařízení (ES) č. 223/2009 o evropské statistice Rozsudek SDEU (velkého senátu) z roku 2008, C-524/06, *Huber v. Bundesrepublik Deutschland*	**Úřední statistika**	Modernizovaná úmluva č. 108 Doporučení o statistických údajích
Směrnice 2014/65/EU o trzích finančních nástrojů Nařízení (EU) č. 648/2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů Nařízení (ES) č. 1060/2009 o ratingových agenturách Směrnice 2007/64/ES o platebních službách na vnitřním trhu	**Finanční údaje**	Modernizovaná úmluva č. 108 Doporučení 90 (19) o ochraně osobních údajů používaných při platebních a jiných souvisejících operacích Rozsudek ESLP z roku 2012, *Michaud v. Francie*, č. 12323/11

V několika případech byly přijaty zvláštní právní nástroje na evropské úrovni s cílem provádět obecná pravidla Modernizované úmluvy č. 108 nebo obecného nařízení o ochraně osobních údajů s větší pozorností věnované konkrétním situacím.

9.1. Elektronická komunikace

Hlavní body

- Zvláštní pravidla o ochraně údajů v oblasti telekomunikací se zvláštním odkazem na telefonní služby jsou uvedena v doporučení RE z roku 1995.
- Zpracování osobních údajů týkajících se poskytování komunikačních služeb je na úrovni EU upraveno směrnicí o soukromí a elektronických komunikacích.
- Důvěrnost elektronických komunikací se týká nejen obsahu komunikace, ale také metadat, jako jsou informace o tom, kdo komunikoval s kým, kdy a jak dlouho, a lokační údaje, například odkud byla data předávána.

Komunikační sítě mají zvýšený potenciál pro neodůvodněný zásah do osobní sféry uživatelů, protože nabízejí obrovské technické možnosti odposlouchávání a zkoumání komunikací uskutečněných pomocí těchto sítí. Proto bylo považováno za nezbytné přijmout zvláštní nařízení o ochraně údajů s cílem zabývat se zvláštními riziky pro uživatele komunikačních služeb.

V roce 1995 vydala **RE** doporučení o ochraně osobních údajů v oblasti telekomunikací, se zvláštním zřetelem k telefonním službám.[917] Podle tohoto doporučení by měly být účely shromažďování a zpracovávání osobních údajů v souvislosti s telekomunikacemi omezeny na: připojení uživatele k síti, zpřístupnění určité telekomunikační služby, pro účely vyúčtování, ověřování, zajišťování optimálního technického provozu a rozvoje sítí a služeb.

Zvláštní pozornost byla rovněž věnována použití komunikačních sítí k zasílání přímých marketingových zpráv. Obecně platí, že přímé marketingové zprávy nemohou být zaslány odběrateli, který se výslovně rozhodl, že je nebude odebírat. Zařízení pro automatické volání pro předávání předem nahraného reklamního sdělení může být použito pouze tehdy, pokud k tomu odběratel udělil výslovný souhlas. Vnitrostátní právo stanoví podrobná pravidla v této oblasti.

Pokud jde o **právní rámec EU**, směrnice o soukromí a elektronických komunikacích byla přijata (po prvním pokusu v roce 1997) v roce 2002 a změněna v roce 2009. Účelem změny bylo doplnit a upravit na míru ustanovení předchozí směrnice o ochraně údajů s ohledem na odvětví telekomunikací.[918]

Uplatňování směrnice o soukromí a elektronických komunikacích je omezeno na komunikační služby ve veřejných komunikačních sítích.

Směrnice o soukromí a elektronických komunikacích rozlišuje tři hlavní kategorie údajů vytvořených v průběhu komunikace:

- údaje, které tvoří obsah zpráv zaslaných během komunikace – tyto údaje jsou přísně důvěrné,

917 Rada Evropy, Výbor ministrů (1995), Doporučení Rec(95)4 členským státům ze dne 7. února 1995 o ochraně osobních údajů v oblasti telekomunikačních služeb, se zvláštním zřetelem k telefonním službám.

918 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, Úř. věst. 2002 L 201 (směrnice o soukromí a elektronických komunikacích) ve znění směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, Úř. věst. 2009 L 337.

- údaje nezbytné pro navázání a udržování komunikace – takzvaná metadata, ve směrnici označovaná jako „údaje o provozu" – například informace o účastnících komunikace, čase a délce trvání komunikace,

- v rámci metadat existují údaje, které se konkrétně týkají umístění komunikačního zařízení, takzvané lokační údaje – tyto údaje jsou současně údaje o místě, kde se nacházejí uživatelé komunikačních zařízení, zejména pokud jde o uživatele mobilních komunikačních zařízení.

Údaje o provozu může používat poskytovatel služeb pouze pro účely fakturace a pro technické poskytování služby. Avšak se souhlasem subjektu údajů mohou být tyto údaje zpřístupněny jiným správcům, kteří nabízejí služby s přidanou hodnotou, jako je poskytování informací s ohledem na místo, kde se nachází uživatel, například o tom, kde je nejbližší stanice metra nebo lékárna nebo jaká je předpověď počasí pro tuto lokalitu.

Podle článku 15 směrnice o soukromí a elektronických komunikacích musí jiný přístup k údajům o komunikacích v elektronických sítích splňovat požadavky na odůvodněný zásah do práva na ochranu údajů, jež jsou stanoveny v čl. 8 odst. 2 EÚLP a stvrzeny v Listině základních práv EU v článcích 8 a 52. Takovýto přístup může zahrnovat přístup za účelem vyšetřování trestných činů.

Změna směrnice o soukromí a elektronických komunikacích z roku 2009[919] zavádí tyto změny:

- Omezení týkající se zasílání e-mailů pro účely přímého marketingu byla rozšířena i na služby krátkých textových zprávy, služby zasílání multimediálních zpráv a jiné druhy podobných aplikací; marketingové e-maily jsou zakázané, ledaže byl získán předchozí souhlas. Bez takového souhlasu je možné se obrátit marketingovými e-maily pouze na předchozí zákazníky, pokud dali svou e-mailovou adresu k dispozici a nevznesli námitky.

919 Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, Úř. věst. 2009 L 337.

- Členským státům byla uložena povinnost poskytovat soudní prostředky nápravy proti porušení zákazu nevyžádaných sdělení.[920]

- Nastavení „cookies“, softwaru, který sleduje a zaznamenává akce uživatele počítače, již není dovoleno bez souhlasu uživatele počítače. Vnitrostátní právo by mělo podrobněji upravit, jak by měl být vyjádřen a získáván souhlas s cílem nabídnout dostatečnou ochranu.[921]

Pokud dojde k porušení zabezpečení v důsledku neoprávněného přístupu, ztráty nebo zničení údajů, musí být neprodleně informován příslušný dozorový úřad. Účastníci musí být také informováni, pokud jim může hrozit újma v důsledku porušení zabezpečení.[922]

Směrnice o uchovávání údajů[923] uložila poskytovatelům komunikačních služeb povinnost uchovávat metadata. Směrnice však byla prohlášena za neplatnou SDEU (pro více podrobností viz oddíl 8.3).

Budoucnost

V lednu 2017 přijala Evropská komise nový návrh nařízení o soukromí a elektronických komunikacích, které má nahradit starou směrnici o soukromí a elektronických komunikacích. Cílem bude i nadále ochrana „základních práv a svobod fyzických a právnických osob při poskytování a využívání služeb elektronických komunikací, a zejména práv na respektování soukromého života a komunikace a ochranu fyzických osob v souvislosti se zpracováním osobních údajů“. Současně má nový návrh zajistit volný pohyb dat elektronických komunikací a služeb elektronických komunikací v rámci Unie.[924] Zatímco obecné nařízení o ochraně osobních údajů se primárně

920 Viz pozměněná směrnice, článek 13.

921 Viz tamtéž, článek 5; viz také pracovní skupina zřízená podle článku 29 (2012), *Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies*, WP 194, Brusel, 7. června 2012.

922 Viz také pracovní skupina zřízená podle článku 29 (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments [Pracovní dokument 01/2011 o platném rámci EU pro porušení zabezpečení osobních údajů a doporučení pro budoucí vývoj politiky]*, WP 184, Brusel, 5. dubna 2011.

923 Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, Úř. věst. 2006 L 105.

924 Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), (COM(2017) 10 final), článek 1.

zaměřuje na článek 8 Listiny základních práv EU, cílem navrhovaného nařízení je začlenit článek 7 Listiny do sekundárního práva EU.

Nařízení by přizpůsobilo ustanovení starší směrnice s ohledem na nové technologie a realitu na trhu a vybudovalo by komplexní a soudržný rámec spolu s obecným nařízením o ochraně osobních údajů. V tomto smyslu by nařízení o soukromí a elektronických komunikacích představovalo *lex specialis* k obecnému nařízení o ochraně osobních údajů a uzpůsobilo by ustanovení obecného nařízení na míru těm datům elektronických komunikací, která představují osobní údaje. Nové nařízení zahrnuje zpracování „dat elektronických komunikací", včetně obsahu a metadat elektronických komunikací, která nejsou nezbytně osobními údaji. Územní působnost je omezena na EU, včetně případů, kdy jsou údaje získané v EU zpracovávány mimo EU, a rozšiřuje se na poskytovatele komunikačních služeb „over the top". To jsou poskytovatelé služeb, kteří poskytují obsah, služby nebo aplikace prostřednictvím internetu bez přímého zapojení operátora sítí nebo poskytovatele internetových služeb. Příkladem takovýchto poskytovatelů může být Skype (hlasové a videohovory), WhatsApp (zasílání zpráv), Google (vyhledávání), Spotify (hudba) nebo Netflix (videoobsah). Na nové nařízení se použijí donucovací mechanismy obecného nařízení o ochraně osobních údajů.

Nařízení o soukromí a elektronických komunikacích má být přijato do 25. května 2018, od kdy bude obecné nařízení o ochraně osobních údajů použitelné ve všech 28 členských státech. To však závisí na dohodě Evropského parlamentu a Rady.[925]

9.2. Údaje v souvislosti se zaměstnáváním

Hlavní body

- Zvláštní pravidla pro ochranu údajů v zaměstnaneckém poměru jsou uvedena v doporučení RE o údajích v souvislosti se zaměstnáváním.
- V obecném nařízení o ochraně osobních údajů jsou zaměstnanecké vztahy výslovně uvedeny pouze v souvislosti se zpracováním citlivých údajů.

925 Pro více informací viz Evropská komise (2017), „Komise navrhuje vysokou úroveň ochrany soukromí ve všech elektronických komunikacích a aktualizuje pravidla ochrany údajů pro orgány EU", tisková zpráva, 10. ledna 2017.

- Platnost souhlasu, který musí být svobodný, jako právního základu pro zpracování údajů o zaměstnancích může být sporná kvůli hospodářské nerovnováze vztahu mezi zaměstnavatelem a zaměstnanci. Je třeba pečlivě posoudit okolnosti souhlasu.

Zpracování údajů v kontextu zaměstnávání se řídí obecnými právními předpisy EU o ochraně osobních údajů. Jedno nařízení[926] se však výslovně zabývá ochranou zpracování osobních údajů ze strany evropských orgánů v kontextu zaměstnávání (kromě jiného). V obecném nařízení o ochraně osobních údajů je zaměstnanecký poměr výslovně uveden v čl. 9 odst. 2, kde se uvádí, že osobní údaje mohou být zpracovávány při plnění povinností nebo vykonávání zvláštních práv správce nebo subjektu údajů v oblasti zaměstnání.

Podle obecného nařízení o ochraně osobních údajů by zaměstnanec měl mít možnost jasně rozlišovat mezi údaji, s jejichž zpracováním/ukládáním svobodně souhlasil, a účely, pro které jsou jeho údaje ukládány. Zaměstnanci by také měli být informováni o svých právech a délce ukládání údajů, než je možné udělit souhlas. Pokud dojde k porušení zabezpečení osobních údajů, u něhož je pravděpodobné, že povede k vysokému riziku pro práva a svobody fyzických osob, musí zaměstnavatel zaměstnanci porušení zabezpečení oznámit. Článek 88 nařízení umožňuje členským státům stanovit konkrétnější pravidla k zajištění ochrany práv a svobod zaměstnanců s ohledem na jejich osobní údaje v souvislosti se zaměstnáním.

Příklad: Ve věci *Worten*[927] údaje zahrnovaly evidenci pracovní doby, ve které byla uvedena denní pracovní doba a doby odpočinku, což představuje osobní údaje. Vnitrostátní právo může uložit zaměstnavateli povinnost zpřístupnit evidenci pracovní doby vnitrostátním orgánům odpovědným za sledování pracovních podmínek. Tím by se umožnil okamžitý přístup k relevantním osobním údajům. Přístup k osobním údajům je však nezbytný k tomu, aby vnitrostátní orgán mohl sledovat dodržování právních předpisů v oblasti pracovních podmínek.[928]

926 Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Úř. věst. 2001 L 8.

927 Rozsudek SDEU ze dne 30. května 2013, C-342/12, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, bod 19.

928 Tamtéž, bod 43.

Pokud jde o **RE**, rozhodnutí o údajích v souvislosti se zaměstnáváním bylo vydáno v roce 1989 a revidováno v roce 2015.[929] Doporučení se týká zpracování osobních údajů pro zaměstnanecké účely v soukromém i veřejném sektoru. Zpracování musí být v souladu s určitými zásadami a omezeními, jako je zásada transparentnosti a konzultace se zástupci zaměstnanců, než budou na pracovišti uvedeny do provozu systémy monitorování. V doporučení se rovněž uvádí, že zaměstnavatelé by měli uplatňovat preventivní opatření, jako jsou filtry, namísto sledování používání internetu ze strany zaměstnanců.

Průzkum nejběžnějších problémů v oblasti ochrany údajů specifických pro oblast zaměstnávání lze nalézt v pracovním dokumentu pracovní skupiny zřízené podle článku 29.[930] Pracovní skupina analyzovala význam souhlasu jako právního základu pro zpracování údajů v souvislosti se zaměstnáváním.[931] Dospěla k závěru, že ekonomická nerovnováha mezi zaměstnavatelem žádajícím o souhlas a zaměstnancem, který souhlas poskytuje, často vyvolá pochybnosti o tom, zda byl souhlas svobodný, či nikoliv. Při posuzování platnosti souhlasu v souvislosti se zaměstnáváním by proto měly být pečlivě zváženy okolnosti, za kterých se spoléhá na souhlas jako na právní základ pro zpracování údajů.

Běžným problémem v oblasti ochrany údajů v nyní obvyklém pracovním prostředí je legitimní míra sledování elektronických komunikací zaměstnanců na pracovišti. Často se uvádí, že tento problém lze snadno vyřešit zákazem soukromého používání komunikačních zařízení na pracovišti. Tento obecný zákaz by však mohl být nepřiměřený a nerealistický. V této souvislosti jsou zvlášť relevantní rozsudky ESLP ve věci *Copland v. Spojené království* a ve věci *Bărbulescu v. Rumunsko*.

Příklad: Ve věci *Copland v. Spojené království*[932] bylo tajně monitorováno používání telefonu, e-mailu a internetu ze strany zaměstnankyně vysoké školy s cílem posoudit, zda nadměrně používala zařízení vysoké školy pro osobní účely. ESLP konstatoval, že telefonní hovory z prostor pracoviště spadají do působnosti pojmu soukromý život a korespondence. Proto tyto hovory a e-maily z pracoviště, jakož i informace získané na základě monitorování

929 Rada Evropy, Výbor ministrů (2015), Doporučení členským státům Rec(2015)5 týkající se zpracování osobních údajů v kontextu zaměstnávání, duben 2015.

930 Pracovní skupina zřízená podle článku 29 (2017), *Stanovisko 2/2017 ke zpracování údajů na pracovišti*, WP 249, Brusel, 8. června 2017.

931 Pracovní skupina zřízená podle článku 29 (2005), *Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995*, WP 114, Brusel, 25. listopadu 2005.

932 Rozsudek ESLP ze dne 3. dubna 2007, *Copland v. Spojené království*, č. 62617/00.

používání internetu pro osobní účely jsou chráněny článkem 8 EÚLP. V případě stěžovatelky neexistovala žádná ustanovení, která by upravovala okolnosti, za nichž by zaměstnavatelé mohli monitorovat používání telefonu, e-mailu a internetu zaměstnanci. Proto zásah nebyl v souladu se zákonem. Soud rozhodl, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Bărbulescu v. Rumunsko*[933] byl stěžovatel propuštěn za používání internetu na svém pracovišti během pracovní doby v rozporu s interními předpisy. Jeho zaměstnavatel monitoroval jeho komunikaci. Během vnitrostátního řízení byly předloženy záznamy zpráv čistě soukromé povahy. ESLP konstatoval, že se použije článek 8, ale ponechal otevřenou otázku, zda restriktivní předpisy zaměstnavatele ponechávaly stěžovateli přiměřené očekávání soukromí. Dospěl však k závěru, že pokyny zaměstnavatele nemohou omezovat soukromý sociální život na pracovišti na nulu.

Pokud jde o skutkovou podstatu, státy, které jsou smluvními stranami, musejí mít široký prostor pro vlastní uvážení při posuzování nutnosti stanovit právní rámec, který bude upravovat podmínky, za nichž by zaměstnavatel mohl regulovat elektronické a jiné komunikace nepracovní povahy ze strany zaměstnanců na pracovišti. Vnitrostátní orgány však musejí zajistit, aby zavedení opatření na sledování korespondence a jiné komunikace ze strany zaměstnavatele, bez ohledu na rozsah a délku trvání těchto opatření, bylo doplněno o vhodné a dostatečné záruky proti zneužití. Stěžejní jsou proporcionalita a procesní záruky před svévolí a ESLP určil řadu faktorů, které byly za daných okolností relevantní. Mezi ně patří mimo jiné rozsah sledování ze strany zaměstnavatele a míra zásahu do soukromí zaměstnance, důsledky pro zaměstnance a to, zda byly stanoveny dostatečné záruky. Kromě toho musí vnitrostátní orgány zajistit, aby zaměstnanec, jehož komunikace byla sledována, měl přístup k opravným prostředkům u soudního orgánu, který má soudní příslušnost určit, alespoň v zásadě, jak byla tato nastíněná kritéria dodržována a zda napadená opatření byla zákonná.

V tomto případě ESLP konstatoval, že došlo k porušení článku 8, protože vnitrostátní orgány nezajistily dostatečnou ochranu práva stěžovatele na respektování jeho soukromého života a korespondence, a proto nedokázaly dosáhnout spravedlivé rovnováhy mezi dotčenými zájmy.

933 Rozsudek ESLP (velkého senátu) ze dne 5. září 2017, *Bărbulescu v. Rumunsko*, č. 61496/08, bod 121.

Podle doporučení RE o zaměstnání by osobní údaje shromažďované pro účely zaměstnávání měly být získávány přímo od konkrétního zaměstnance.

Osobní údaje shromažďované pro účely náboru musí být omezeny na to, co je nezbytné ke zhodnocení vhodnosti uchazečů a jejich kariérního potenciálu.

Doporučení rovněž výslovně zmiňuje údaje z hodnocení týkajícího se výkonnosti a potenciálu jednotlivých zaměstnanců. Údaje z hodnocení musí být založeny na spravedlivém a upřímném hodnocení a nesmí být formulovány urážlivě. Tato povinnost je dána zásadou korektního zpracování údajů a přesnosti údajů.

Zvláštním aspektem práva v oblasti ochrany údajů ve vztazích mezi zaměstnavatelem a zaměstnancem je úloha zástupců zaměstnanců. Tito zástupci mohou získat osobní údaje zaměstnanců pouze v rozsahu, v jakém je to nezbytné, aby mohli zastupovat zájmy zaměstnanců, nebo pokud jsou tyto údaje nezbytné ke splnění povinností stanovených v kolektivních smlouvách nebo k dohlížení na plnění těchto povinností.

Citlivé osobní údaje shromážděné pro účely zaměstnávání mohou být zpracovány pouze v konkrétních případech a podle záruk stanovených ve vnitrostátním právu. Zaměstnavatelé mohou požádat zaměstnance nebo uchazeče o zaměstnání o informace o jejich zdravotním stavu nebo mohou provést lékařskou prohlídku pouze tehdy, pokud je to nezbytné. Může se jednat o tyto případy: jejich vhodnost pro dané zaměstnání, splnění požadavků preventivního lékařství, zajištění životně důležitých zájmů subjektu údajů nebo jiných zaměstnanců a jednotlivců, umožnění poskytnutí sociálních dávek nebo odpověď na žádost soudu. Zdravotní údaje nesmějí být shromažďovány z jiných zdrojů, ale pouze od dotčeného zaměstnance, s výjimkou případů, kdy byl získán výslovný a informovaný souhlas nebo kdy to stanoví vnitrostátní právo.

Podle doporučení o zaměstnání by zaměstnavatelé měli být informováni o účelu zpracování svých osobních údajů, druhu shromažďovaných osobních údajů, o subjektech, jimž jsou údaje pravidelně oznamovány, a o účelu a právním základu pro toto zpřístupnění. Přístup k elektronické komunikaci na pracovišti je možný pouze z důvodu bezpečnosti a jiných oprávněných důvodů a tento přístup je možný pouze poté, co byli zaměstnanci informováni, že zaměstnavatel může mít přístup k tomuto druhu komunikace.

Zaměstnanci musejí mít právo na přístup ke svým údajům v souvislosti se zaměstnáváním, jakož i právo na opravu nebo výmaz. Pokud se zpracovávají údaje o hodnocení, musí zaměstnanci navíc mít právo hodnocení napadnout. Tato práva však mohou být dočasně omezena za účelem interního vyšetřování. Pokud bude zaměstnanci odepřen přístup, oprava nebo výmaz osobních údajů v souvislosti se zaměstnáváním, musí vnitrostátní právní řád stanovit vhodné postupy, jimiž lze toto odepření napadnout.

9.3. Zdravotní údaje

Hlavní body

- Lékařské údaje jsou citlivé údaje, a proto se těší zvláštní ochraně.

Osobní údaje týkající se zdraví subjektu údajů se podle čl. 9 odst. 1 obecného nařízení o ochraně osobních údajů a podle článku 6 Modernizované úmluvy č. 108 považují za citlivé údaje. Zdravotní údaje tudíž podléhají přísnějšímu režimu zpracování údajů než údaje, které citlivé nejsou. Obecné nařízení o ochraně osobních údajů zakazuje zpracování „osobních údajů o zdravotním stavu" (čímž se rozumí „veškeré údaje související se zdravotním stavem subjektu údajů, které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů")[934], jakož i genetických a biometrických údajů, ledaže čl. 9 odst. 2 toto zpracování povoluje. Oba druhy údajů byly přidány na seznam „zvláštních kategorií údajů".[935]

Příklad: Ve věci *Z v. Finsko* spáchal bývalý manžel stěžovatelky, který byl nakažen virem HIV, řadu sexuálně motivovaných trestných činů.[936] Následně byl odsouzen za zabití z toho důvodu, že vědomě vystavil své oběti riziku nákazy virem HIV. Vnitrostátní soud nařídil, aby úplné znění rozsudku a dokumentace případu byly důvěrné po dobu 10 let, a to navzdory žádostem stěžovatelky o delší lhůtu pro zachování důvěrnosti. Odvolací soud tyto

934 Obecné nařízení o ochraně osobních údajů, 35. bod odůvodnění.

935 Tamtéž, článek 2.

936 Rozsudek ESLP ze dne 25. února 1997, *Z v. Finsko*, č. 22009/93, body 94 a 112; viz také rozsudek ESLP ze dne 27. srpna 1997, *M.S. v. Švédsko*, č. 20837/92; rozsudek ESLP ze dne 10. října 2006, *L.L. v. Francie*, č. 7508/02; rozsudek ESLP ze dne 17. července 2008, *I v. Finsko*, č. 20511/03; rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další v. Slovensko*, č. 32881/04; rozsudek ESLP ze dne 2. června 2009, *Szuluk v. Spojené království*, č. 36936/05.

žádosti zamítl a jeho rozsudek obsahoval celé jméno jak stěžovatelky, tak jejího bývalého manžela. ESLP rozhodl, že zásah není považován za nezbytný v demokratické společnosti, protože ochrana lékařských údajů má zásadní význam pro požívání práva na respektování soukromého a rodinného života, zejména pokud jde o informace o nákaze virem HIV vzhledem ke stigmatu, který je s tímto onemocněním v řadě společností spojen. Proto soud dospěl k závěru, že umožnění přístupu k rozsudku odvolacího soudu, který obsahoval totožnost stěžovatelky a její zdravotní stav, pouhých 10 let po vydání rozsudku by bylo porušením článku 8 EÚLP.

Podle **práva EU** umožňuje čl. 9 odst. 2 písm. h) obecného nařízení o ochraně osobních údajů zpracování lékařských údajů, je-li nezbytné pro účely preventivního lékařství, lékařské diagnostiky, poskytování péče či léčby nebo řízení služeb zdravotní péče. Zpracování je však přípustné pouze tehdy, pokud je provádí zdravotník podléhající povinnosti zachovávat lékařské tajemství nebo jiná osoba s rovnocennou povinností.

V rámci **práva RE** uplatňuje doporučení RE o zdravotních údajích z roku 1997 podrobněji zásady Úmluvy č. 108 na zpracování údajů v lékařské oblasti.[937] Navrhovaná pravidla jsou v souladu s pravidly obecného nařízení o ochraně osobních údajů, pokud jde o legitimní účely zpracování lékařských údajů, nezbytné povinnosti osob používající lékařské údaje zachovávat lékařské tajemství a práva subjektů údajů na transparentnost a přístup, opravu a výmaz. Navíc lékařské údaje, které jsou v souladu se zákonem zpracovávány zdravotníky, nesmějí být předány donucovacím orgánům, ledaže jsou stanoveny „dostatečné záruky zabraňující zpřístupnění údajů v rozporu s respektováním [...] soukromého života zaručeného článkem 8 EÚLP".[938] Vnitrostátní právo musí být také „formulováno s dostatečnou přesností a poskytovat dostatečnou právní ochranu před svévolí".[939]

Kromě toho doporučení o zdravotních údajích obsahuje zvláštní ustanovení o lékařských údajích nenarozených dětí a osob nezpůsobilých k právním úkonům a o zpracování genetických údajů. Výslovně se uznává, že vědecký výzkum je důvodem pro uchovávání údaje déle, než je nezbytné, ačkoliv k tomu je obvykle zapotřebí

937 Rada Evropy, Výbor ministrů (1997), Doporučení Rec(97)5 členským státům o ochraně zdravotních údajů, 13. února 1997. Upozorňuje, že toto doporučení je v současnosti přezkoumáváno.

938 Rozsudek ESLP ze dne 6. června 2013, *Assenov a další v. Bulharsko*, č. 1585/09, bod 53. Viz také rozsudek ESLP ze dne 25. listopadu 2008, *Biriuk v. Litva*, č. 23373/03.

939 Rozsudek ESLP ze dne 29. dubna 2014, *L.H. v. Lotyšsko*, č. 52019/07, bod 59.

anonymizace. Článek 12 doporučení o zdravotních údajích navrhuje podrobnou úpravu situací, kdy výzkumní pracovníci potřebují osobní údaje a anonymizované údaje nestačí.

Pseudonymizace může být vhodným prostředkem k uspokojení vědeckých potřeb a současně k ochraně zájmů dotčených pacientů. Pojetí pseudonymizace v souvislosti s ochranou údajů je podrobněji vysvětleno v oddíle 2.1.1.

Na zpracování údajů v lékařské oblasti se také použije doporučení RE z roku 2016 týkající se údajů zjištěných pomocí genetických testů.[940] Toto doporučení má velký význam pro elektronické zdravotnictví, kde se IKT používá k usnadnění lékařské péče. Příkladem může být zaslání výsledků rodičovského testu pacienta od jednoho poskytovatele zdravotní péče jinému. Cílem tohoto doporučení je ochránit práva osob, jejichž osobní údaje se zpracovávají pro pojistné účely, s cílem pojistit se proti rizikům souvisejícím se zdravím dané osoby, její fyzickou nedotknutelností, věkem nebo úmrtím. Pojišťovny musejí odůvodnit zpracování zdravotních údajů a to by mělo být přiměřené povaze a významu příslušného rizika. Zpracování těchto údajů závisí na souhlasu daného subjektu. Pojišťovny by také měly mít zavedené záruky pro ukládání zdravotních údajů.

Klinická hodnocení – která zahrnují posouzení nových léčivých přípravků na pacienty v dokumentovaném prostředí výzkumu – mají značné důsledky pro ochranu údajů. Klinická hodnocení humánních léčivých přípravků jsou upravena nařízením Evropského parlamentu a Rady (EU) č. 536/2014 ze dne 16. dubna 2014 o klinických hodnoceních humánních léčivých přípravků a o zrušení směrnice 2001/20/ES (nařízení o klinických hodnoceních).[941] Toto jsou hlavní prvky nařízení o klinických hodnoceních:

- zefektivněný postup podávání žádostí prostřednictvím portálu EU,[942]
- lhůty pro posouzení žádosti o klinická hodnocení,[943]

940 Rada Evropy, Výbor ministrů (2016), Doporučení Rec(2016)8 členským státům týkající se zpracování osobních zdravotních údajů pro pojistné účely, včetně údajů pocházejících z genetických testů, 26. října 2016.

941 Nařízení Evropského parlamentu a Rady (EU) č. 536/2014 ze dne 16. dubna 2014 o klinických hodnoceních humánních léčivých přípravků a o zrušení směrnice 2001/20/ES (nařízení o klinických hodnoceních), Úř. věst. 2014 L 158.

942 Nařízení o klinických hodnoceních, čl. 5 odst. 1.

943 Tamtéž, čl. 5 odst. 2 až 5.

- začlenění etické komise do hodnocení v souladu s právem členských států (a evropským právem, které definuje příslušné lhůty)[944] a

- větší transparentnost klinických hodnocení a jejich výsledků.[945]

Obecné nařízení o ochraně osobních údajů upřesňuje, že pro účely udělení souhlasu s účastí na činnostech vědeckého výzkumu v rámci klinických hodnocení se použije nařízení (EU) č. 536/2014.[946]

Na úrovni EU se v současnosti projednává řada dalších legislativních a jiných iniciativ týkajících se osobních údajů ve zdravotnictví.[947]

Elektronické zdravotní záznamy

Elektronické zdravotní záznamy se definují jako „komplexní lékařský záznam nebo podobná dokumentace o minulém a současném stavu tělesného a duševního zdraví fyzické osoby v elektronické podobě, který zajišťuje snadnou dostupnost těchto údajů pro léčbu a jiné s ní úzce související účely".[948] Elektronické zdravotní záznamy jsou elektronickou verzí pacientovy anamnézy a mohou zahrnovat klinické údaje týkající se těchto jednotlivců, například lékařskou anamnézu, potíže a onemocnění, léčivé přípravky a léčebné postupy, jakož i laboratorní výsledky a zprávy a výsledky a zprávy z vyšetření. Tyto elektronické soubory, které mohou mít nejrůznější podobu – od celkových záznamů až po pouhé výpisy nebo shrnutí –, si může prohlížet praktický lékař, lékárník a jiní zdravotničtí pracovníci. O těchto zdravotních záznamech pojednává i koncepce „elektronického zdraví".

Příklad: Pan A uzavřel pojistku se společností B (pojišťovnou). Pojišťovna bude shromažďovat určité zdravotní informace od pana A, například o aktuálních zdravotních potížích a onemocněních. Pojišťovna by měla ukládat osobní zdravotní údaje pana A odděleně od ostatních údajů. Rovněž musí ukládat

944 Tamtéž, čl. 2 odst. 2 bod 11.

945 Tamtéž, čl. 9 odst. 1 a 67. bod odůvodnění.

946 Obecné nařízení o ochraně osobních údajů, 156. a 161. bod odůvodnění.

947 EIOÚ (2013), *Stanovisko Evropského inspektora ochrany údajů ke sdělení Komise „Akční plán pro elektronické zdravotnictví na období 2012–2020 – inovativní zdravotní péče pro 21. století"*, Brusel, 27. března 2013.

948 Doporučení Komise ze dne 2. července 2008 o přeshraniční interoperabilitě systémů elektronických zdravotních záznamů, bod 3 písm. c).

osobní zdravotní údaje odděleně od jiných osobních údajů. To znamená, že ke zdravotním údajům pana A bude mít přístup pouze osoba zpracovávající případ pana A.

V souvislosti s elektronickými zdravotními spisy však vyvstávají určité otázky týkající se ochrany údajů, například ohledně jejich přístupnosti, řádného uchovávání a přístupu ze strany subjektu údajů.

Kromě doporučení o elektronických zdravotních záznamech zveřejnila Evropská komise dne 10. dubna 2014 zelenou knihu o mobilním zdravotnictví („mHealth"), ve které vyjádřila názor, že mobilní zdravotnictví představuje novou a rychle se vyvíjející oblast, která může přispět k transformaci zdravotní péče a zvýšit její kvalitu a účinnost. Tento pojem zahrnuje lékařskou péči a péči o veřejné zdraví za podpory mobilních zařízení, jako jsou mobilní telefony, přístroje pro monitorování pacientů, osobní digitální asistenti a další bezdrátová zařízení, ale také aplikace (například aplikace týkající se dobré kondice), které se mohou připojit ke zdravotnickým prostředkům či senzorům.[949] V dokumentu se nastiňují rizika pro ochranu osobních údajů, které by rozvoj mobilního zdravotnictví mohl zahrnovat, a stanoví se, že vzhledem k citlivé povaze zdravotních údajů by vývoj měl obsahovat konkrétní a přiměřené záruky bezpečnosti údajů pacientů, jako je šifrování a vhodné ověřovací mechanismy pro pacienty, které zmírní bezpečnostní rizika. Dodržování pravidel ochrany osobních údajů, včetně povinnosti informovat subjekt údajů, zabezpečení údajů a zásady zákonného zpracování osobních údajů, proto má zásadní význam pro budování důvěryhodnosti řešení v oblasti mHealth.[950] Za tímto účelem vypracovalo dané odvětví kodex chování založený na příspěvcích od širokého spektra zúčastněných stran, včetně zástupců s odbornými znalostmi v oblasti ochrany údajů, seberegulace a společné regulace, IKT a zdravotní péče.[951] V době psaní této příručky byl návrh kodexu chování předložen k připomínkování pracovní skupině pro ochranu údajů zřízené podle článku 29 a čeká se na jeho formální schválení.

949 Evropská komise (2014), *Zelená kniha o mobilním zdravotnictví („mHealth")*, COM(2014) 219 final, Brusel, 10. dubna 2014.

950 Tamtéž, s. 8.

951 Návrh kodexu chování v souvislosti s ochranou soukromí u mobilních zdravotních aplikací, 7. června 2016.

9.4. Zpracování údajů pro výzkumné a statistické účely

Hlavní body

- Údaje shromážděné pro účely vědeckého či historického výzkumu nebo pro statistické účely nesmějí být použity pro žádný jiný účel.
- Údaje shromážděné oprávněným způsobem pro jakýkoliv účel mohou být dále použity pro účely vědeckého či historického výzkumu nebo pro statistické účely, pokud jsou zajištěny dostatečné záruky. Za tímto účelem mohou tyto záruky poskytnout anonymizace nebo pseudonymizace před předáním údajů třetím straním.

Právo EU umožňuje zpracování údajů pro účely vědeckého či historického výzkumu nebo pro statistické účely, pokud jsou zavedeny vhodné záruky pro práva a svobody subjektů údajů. Mezi ně může patřit i pseudonymizace.[952] Právo EU nebo členského státu může stanovit určité odchylky od práv subjektů údajů, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění legitimního účelu výzkumu.[953] Je možné zavést odchylky od práva na přístup subjektu údajů, práva na opravu, práva na omezení zpracování a práva vznést námitku.

Ačkoliv údaje shromážděné správcem v souladu s právními předpisy za jakýmkoliv účelem mohou být opětovně použity tímto správcem pro vlastní statistické účely a účely vědeckého nebo historického výzkumu, údaje by měly být anonymizovány nebo by měly být předmětem opatření, jako je pseudonymizace, a to v závislosti na kontextu, před předáním údajů třetí straně pro účely vědeckého či historického výzkumu nebo pro statistické účely, ledaže s tím subjekt údajů souhlasil nebo pokud to výslovně stanoví vnitrostátní právo. Pseudonymizované údaje se i nadále řídí obecným nařízením o ochraně osobních údajů, na rozdíl od anonymních údajů.[954]

Nařízení tudíž výzkumu přiznává zvláštní zacházení, pokud jde o obecná pravidla ochrany údajů, s cílem zabránit omezení rozvoje výzkumu a postupovat v souladu s cílem vytvořit evropský výzkumný prostor, jak je stanoveno v článku 179 SFEU. Umožňuje široký výklad zpracování osobních údajů pro účely vědeckého výzkumu, včetně technologického vývoje a demonstrací, základního výzkumu, aplikovaného

952 Obecné nařízení o ochraně osobních údajů, čl. 89 odst. 1.

953 Tamtéž, čl. 89 odst. 2.

954 Tamtéž, 26. bod odůvodnění.

výzkumu a výzkumu financovaného ze soukromých zdrojů. Uznává rovněž význam shromažďování údajů v rejstřících pro účely výzkumu a možné potíže při plné identifikaci následného účelu zpracování osobních údajů pro účely vědeckého výzkumu v době shromažďování údajů.[955] Z tohoto důvodu nařízení umožňuje zpracování údajů pro tyto účely bez souhlasu subjektů údajů, pokud jsou zavedeny příslušné záruky.

Důležitým příkladem používání údajů pro statistické účely jsou úřední statistiky získané vnitrostátními a unijními statistickými úřady v souladu s právními předpisy členských států a EU o úřední statistice. Podle těchto právních předpisů jsou občané a podniky obvykle povinny zpřístupňovat údaje příslušným statistickým orgánům. Úředníci zaměstnaní ve statistických úřadech jsou vázáni zvláštní povinností zachovávat služební tajemství, kterou je třeba řádně dodržovat, protože je zásadní pro vysokou úroveň důvěry občanů, která je nezbytná, mají-li být údaje statistickým úřadům zpřístupňovány.[956]

Nařízení (ES) č. 223/2009 o evropské statistice (dále jen „nařízení o evropské statistice“) obsahuje základní pravidla pro ochranu údajů v kontextu úředních statistik, a proto může být také považováno za relevantní pro ustanovení týkající se úředních statistik na vnitrostátní úrovni.[957] Nařízení zavádí zásadu, že činnost v oblasti úřední statistiky musí mít dostatečně jasný právní základ.[958]

Příklad: Ve věci *Huber v. Bundesrepublik Deutschland*[959] si rakouský obchodník, který se přestěhoval do Německa, stěžoval, že shromažďování a uchovávání osobních údajů cizích státních příslušníků ze strany německých orgánů v centrálním registru (AZR) také pro statistické účely je v rozporu s jeho právy

955 Tamtéž, 33., 157. a 159. bod odůvodnění.

956 Tamtéž, článek 90.

957 Nařízení Evropského parlamentu a Rady (ES) č. 223/2009 ze dne 11. března 2009 o evropské statistice a zrušení nařízení (ES, Euratom) č. 1101/2008 o předávání údajů, na které se vztahuje statistická důvěrnost, Statistickému úřadu Evropských společenství, nařízení Rady (ES) č. 322/97 o statistice Společenství a rozhodnutí Rady 89/382/EHS, Euratom, kterým se zřizuje Výbor pro statistické programy Evropských společenství, Úř. věst. 2009 L 87, ve znění nařízení Evropského parlamentu a Rady (EU) 2015/759 ze dne 29. dubna 2015, kterým se mění nařízení (ES) č. 223/2009 o evropské statistice, Úř. věst. 2015 L 123.

958 Tato zásada má být podrobně rozpracována v Kodexu evropské statistiky Eurostatu, který má v souladu s článkem 11 nařízení o evropské statistice poskytnout etické pokyny, jak provádět úřední statistiku, včetně ohleduplného používání osobních údajů.

959 Rozsudek SDEU (velkého senátu) ze dne 16. prosince 2008, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*; viz zejména bod 68.

podle směrnice o ochraně údajů. Vzhledem k tomu, že směrnice 95/46/ES má zajistit rovnocennou úroveň ochrany ve všech členských státech, SDEU rozhodl, že v zájmu zajištění vysoké úrovně ochrany v EU nemůže mít pojem nezbytnost uvedený v čl. 7 písm. e) rozdílný obsah v jednotlivých členských státech. Jedná se tedy o autonomní pojem, který musí být vykládán tak, aby plně odpovídal cíli směrnice 95/46/ES. SDEU konstatoval, že pro statistické účely by měly být požadovány pouze anonymní informace, a rozhodl, že německý registr nebyl slučitelný s požadavky nezbytnosti podle čl. 7 písm. e).

V kontextu **RE** je možné další zpracování údajů provádět pro účely vědeckého či historického výzkumu či pro statistické účely, pokud existuje veřejný zájem, a musí podléhat vhodným zárukám.[960] Práva subjektů údajů mohou být také omezena při zpracování údajů pro statistické účely, pokud nelze rozpoznat riziko porušení práv a svobod těchto subjektů.[961]

Doporučení o statistických údajích vydané v roce 1997 pojednává o provádění statistické činnosti ve veřejném a soukromém sektoru.[962]

Údaje shromážděné správcem pro statistické účely nesmějí být použity pro žádný jiný účel. Údaje shromážděné pro jiné než statistické účely budou dostupné pro další statistické využití. Doporučení o statistických údajích rovněž umožňuje předávání údajů třetím stranám, jsou-li předávány výlučně pro statistické účely. V těchto případech by se strany měly dohodnout a sepsat rozsah oprávněného dalšího užívání pro statistické účely. Jelikož tímto není možné nahradit souhlas subjektu údajů – je-li to zapotřebí –, musí existovat dostatečné záruky stanovené ve vnitrostátním právu, které minimalizují rizika zneužití osobních údajů, jako je povinnost anonymizovat nebo pseudonymizovat údaje před předáním.

Pracovníci v oblasti statistického výzkumu musejí být vázáni zvláštní povinností zachovávat služební tajemství – jak je obvyklé v případě úřední statistiky – v souladu s vnitrostátním právem. Tato povinnost musí být rozšířena na tazatele a další osoby shromažďující osobní údaje, pokud jsou zaměstnáni v oblasti shromažďování údajů od subjektů údajů nebo jiných osob.

960 Modernizovaná úmluva č. 108, čl. 5 odst. 4 písm. b).

961 Tamtéž, čl. 11 odst. 2.

962 Rada Evropy, Výbor ministrů (1997), Doporučení Rec(97)18 členským státům o ochraně osobních údajů shromažďovaných a zpracovávaných pro statistické účely, 30. září 1997.

Pokud statistický průzkum používající osobní údaje není povolen zákonem, je možné, že subjekty údajů budou muset udělit souhlas s využitím svých údajů, má-li být toto využití legitimní, nebo budou muset získat příležitost vznést námitku. Pokud jsou osobní údaje shromážděny tazateli pro statistické účely, musejí být dotazované osoby jasně informovány o tom, zda je poskytování údajů podle vnitrostátního práva povinné, či nikoliv.

Pokud není možné provést statistický průzkum za použití anonymních údajů a jsou zapotřebí osobní údaje, musí být údaje shromážděné za tímto účelem anonymizovány, jakmile to bude možné. Výsledky statistického průzkumu přinejmenším nesmí umožňovat identifikaci jakýchkoliv subjektů údajů, ledaže by tato identifikace zjevně nepředstavovala žádné riziko.

Po provedení statistické analýzy by měly být použité osobní údaje buď smazány, nebo anonymizovány. V takovýchto případech doporučení o statistických údajích uvádí, že identifikační údaje musí být uloženy odděleně od jiných osobních údajů. To například znamená, že buď šifrovací klíč, nebo seznam obsahující identifikační synonyma musejí být uloženy odděleně od jiných údajů.

9.5. Finanční údaje

Hlavní body

- Ačkoliv se finanční údaje podle Modernizované úmluvy č. 108 nebo obecného nařízení o ochraně osobních údajů nepovažují za citlivé údaje, jejich zpracování vyžaduje zvláštní záruky k zajištění přesnosti a bezpečnosti údajů.
- Zejména elektronické platební systémy vyžadují zabudovanou ochranu údajů, tj. záměrnou a standardní ochranu osobních údajů.
- V této oblasti mohou vyvstat zvláštní problémy v oblasti ochrany, protože je nutné mít zavedené vhodné ověřovací mechanismy.

Příklad: Ve věci *Michaud v. Francie*[963] stěžovatel, francouzský advokát, napadl svou povinnost podle francouzského práva oznamovat podezření týkající se možných činností praní peněz ze strany svých klientů. ESLP konstatoval, že povinnost, aby advokáti oznamovali správním orgánům informace týkající se jiné osoby, se kterými se seznámili při výměně informací v rámci své profese, představuje zásah do práva advokátů na respektování jejich korespondence a soukromého života podle článku 8 EÚLP, protože tato koncepce zahrnuje činnosti profesní a obchodní povahy. Zásah byl však v souladu se zákonem a sledoval legitimní cíl, totiž zabránit narušení veřejného pořádku a trestné činnosti. Jelikož advokáti podléhají povinnosti oznamovat podezřelou činnost pouze za velmi konkrétních okolností, ESLP rozhodl, že tato povinnost je přiměřená. Dospěl k závěru, že nedošlo k porušení článku 8.

Příklad: Ve věci *M. N. a další v. San Marino*[964] stěžovatel, italský občan, uzavřel fiduciární dohodu s vyšetřovanou společností. Tím se rozumí, že společnost byla prohledávána a byly zajištěny kopie (elektronické) dokumentace. Stěžovatel podal stížnost sanmarinskému soudu, ve které uváděl, že neexistuje žádná spojitost mezi ním a domnělou trestnou činností. Soud však jeho stížnost prohlásil za nezpůsobilou, protože nebyl „zúčastněnou stranou". ESLP rozhodl, že stěžovatel byl významně znevýhodněn, pokud jde o soudní ochranu, ve srovnání se „zúčastněnou stranou", přesto však jeho údaje byly předmětem operací prohledávání a zajišťování. Soud tedy rozhodl, že došlo k porušení článku 8.

Příklad: Ve věci *G.S.B. v. Švýcarsko*[965] byly údaje o bankovním účtu stěžovatele zaslány daňovým orgánům USA na základě dohody o správní spolupráci mezi Švýcarskem a USA. ESLP konstatoval, že předání nebylo v rozporu s článkem 8 EÚLP, protože zásah do stěžovatelova práva na soukromí byl stanoven zákonem, sledoval legitimní cíl a byl přiměřený vzhledem k dotčenému veřejnému zájmu.

Uplatňování obecného právního rámce ochrany údajů (jak stanoví Úmluva č. 108) na oblast plateb bylo rozvinuto **RE** v doporučení Rec(90)19 z roku 1990.[966] Dopo-

963 Rozsudek ESLP ze dne 6. prosince 2012, *Michaud v. Francie*, č. 12323/11. Viz také rozsudek ESLP ze dne 16. prosince 1992, *Niemietz v. Německo*, č. 13710/88, bod 29, a rozsudek ESLP ze dne 25. června 1997, *Halford v. Spojené království*, č. 20605/92, bod 42.

964 Rozsudek ESLP ze dne 7. července 2015, *M.N. a další v. San Marino*, č. 28005/12.

965 Rozsudek ESLP ze dne 22. prosince 2015, *G.S.B. v. Švýcarsko*, č. 28601/11.

966 Rada Evropy, Výbor ministrů (1990), Doporučení Rec(90)19 členským státům o ochraně osobních údajů používaných při platebních a jiných souvisejících operacích, 13. září 1990.

ručení objasňuje rozsah zákonného shromažďování a používání údajů v souvislosti s platbami, zejména prostřednictvím platebních karet. Rovněž poskytuje vnitrostátním zákonodárcům podrobná doporučení týkající se pravidel pro zpřístupňování údajů o platbách třetím stranám, dále ohledně lhůt pro uchovávání údajů, transparentnosti, bezpečnosti údajů a přeshraničních tocích údajů a o dohledu a opravných prostředcích. RE rovněž vypracovala stanovisko k předávání daňových údajů[967], které stanoví doporučení a problémy, které je třeba zohlednit při předávání daňových údajů.

ESLP umožňuje předávání finančních údajů – konkrétně údajů o bankovních účtech jednotlivce – podle článku 8 EÚLP, pokud je to stanoveno zákonem, sleduje legitimní cíl a je to přiměřené vzhledem k dotčenému veřejnému zájmu.[968]

Pokud jde o **právo EU**, elektronické platební systémy, které zahrnují zpracování osobních údajů, musí být v souladu s obecným nařízením o ochraně osobních údajů. Tyto systémy proto musí zajišťovat záměrnou a standardní ochranu osobních údajů. Záměrná ochrana osobních údajů ukládá správci povinnost zavést vhodná technická a organizační opatření s cílem provést zásady ochrany údajů. Standardní ochrana osobních údajů znamená, že správce musí zajistit, že standardně se zpracovávají pouze ty osobní údaje, které jsou nezbytné pro daný účel (viz oddíl 4.4). Pokud jde o finanční údaje, SDEU rozhodl, že předané daňové údaje mohou představovat osobní údaje.[969] Pracovní skupina pro ochranu údajů zřízená podle článku 29 vydala související pokyny pro členské státy, které obsahují kritéria k zajištění souladu s pravidly ochrany údajů při automatické výměně osobních údajů pro daňové účely automatickými prostředky.[970] Kromě toho byla zavedena řada právních nástrojů s cílem regulovat finanční trhy a aktivity úvěrových institucí a investičních firem.[971] Další

967 Rada Evropy, Poradní výbor k Úmluvě č. 108 (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes [Stanovisko k důsledkům mechanismů pro automatické mezistátní výměny údajů pro správní a daňové účely, pokud jde o ochranu údajů], 4. června 2014.

968 Rozsudek ESLP ze dne 22. prosince 2015, *G.S.B. v. Švýcarsko*, č. 28601/11.

969 Rozsudek SDEU ze dne 1. října 2015, C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*, bod 29.

970 Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29 (2015), Prohlášení k automatickým mezistátním výměnám osobních údajů pro daňové účely, 14/EN WP 230.

971 Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU, Úř. věst. 2014 L 173; nařízení Evropského parlamentu a Rady (EU) č. 600/2014 ze dne 15. května 2014 o trzích finančních nástrojů a o změně nařízení (EU) č. 648/2012, Úř. věst. 2014 L 173; směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES, Úř. věst. 2013 L 176.

právní nástroje pomáhají bojovat proti obchodování zasvěcených osob a manipulaci s trhem.[972] Hlavními oblastmi, které mají dopad na ochranu údajů, jsou:

- uchovávání záznamů o finančních transakcích,
- předávání osobních údajů třetím zemím,
- zaznamenávání telefonních hovorů nebo elektronické komunikace, včetně pravomoci příslušných orgánů vyžádat si záznamy o telefonních hovorech a datových přenosech,
- zpřístupnění osobních informací, včetně zveřejnění sankcí,
- dohledové a vyšetřovací pravomoci příslušných orgánů, včetně inspekcí na místě a vstupu do soukromých prostor za účelem zajištění dokumentů,
- mechanismy pro oznamování porušení předpisů, tj. režimy pro oznamování (whistleblowing), a
- spolupráce mezi příslušnými orgány členských států a Evropským orgánem pro cenné papíry a trhy (ESMA).

Rovněž jsou zvlášť ošetřeny další otázky v těchto oblastech, včetně shromažďování údajů o finančním statusu subjektů údajů[973] nebo přeshraničních plateb bankovními převody, které nevyhnutelně vedou k tokům osobních údajů.[974]

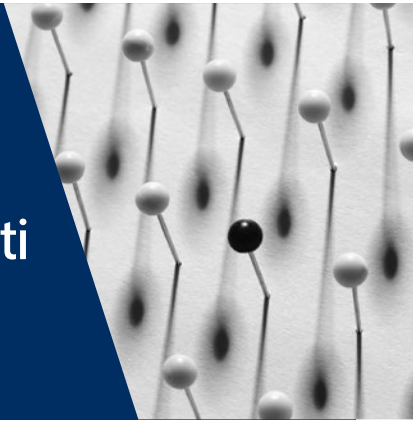
---

972 Nařízení Evropského parlamentu a Rady (EU) č. 596/2014 ze dne 16. dubna 2014 o zneužívání trhu (nařízení o zneužívání trhu) a o zrušení směrnice Evropského parlamentu a Rady 2003/6/ES a směrnic Komise 2003/124/ES, 2003/125/ES a 2004/72/ES, Úř. věst. 2014 L 173.

973 Nařízení Evropského parlamentu a Rady (ES) č. 1060/2009 ze dne 16. září 2009 o ratingových agenturách, Úř. věst. 2009 L 302, které bylo naposledy pozměněno směrnicí Evropského parlamentu a Rady 2014/51/EU ze dne 16. dubna 2014, kterou se mění směrnice 2003/71/ES a 2009/138/ES a nařízení (ES) č. 1060/2009, (EU) č. 1094/2010 a (EU) č. 1095/2010 s ohledem na pravomoci Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění) a Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), Úř. věst. 2014 L 153; a nařízením Evropského parlamentu a Rady (EU) č. 462/2013 ze dne 21. května 2013, kterým se mění nařízení (ES) č. 1060/2009 o ratingových agenturách, Úř. věst. 2013 L 146.

974 Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES, Úř. věst. 2007 L 319, ve znění směrnice Evropského parlamentu a Rady 2009/111/ES ze dne 16. září 2009, kterou se mění směrnice 2006/48/ES, 2006/49/ES a 2007/64/ES, pokud jde o banky přidružené k ústředním institucím, některé položky kapitálu, velkou angažovanost, režimy dohledu a krizové řízení, Úř. věst. 2009 L 302.

10 Novodobé výzvy v oblasti ochrany osobních údajů



Pro digitální věk nebo věk informačních technologií je typické rozšířené používání počítačů, internetu a digitálních technologií. Zahrnuje shromažďování a zpracovávání obrovského objemu údajů, včetně osobních. Shromažďování a zpracování osobních údajů v globalizované ekonomice znamená, že roste objem přeshraničních datových toků. Toto zpracování může přinést významné a viditelné přínosy pro každodenní život: vyhledávače usnadňují přístup ke značnému množství informací a znalostí, služby vytváření sociálních sítí umožňují lidem po celém světě komunikovat, vyjadřovat názory a mobilizovat podporu pro sociální, environmentální a politická témata a podniky a spotřebitelé pak mají výhody z účinných a účelných technik marketingu, které jsou impulzem pro hospodářství. Technologie a zpracování osobních údajů jsou také nepostradatelnými nástroji pro státní orgány v boji proti trestné činnosti a terorismu. Podobně data velkého objemu – shromažďování, ukládání a analýza velkého množství informací s cílem určit vzorce a predikovat chování – „mohou být zdroje významné hodnoty pro společnost, zvýšit produktivitu, výkonnost veřejného sektoru a sociální participaci".[975]

Navzdory mnoha přínosům představuje digitální věk také výzvy pro ochranu soukromí a údajů, protože se shromažďují obrovská množství osobních informací a zpracovávají se stále složitějšími a netransparentnějšími postupy. Technologický pokrok přinesl rozvoj masivních souborů dat, které je možné snadno vzájemně ověřovat a dále analyzovat s cílem najít vzorce chování nebo za účelem přijetí rozhodnutí

975 Rada Evropy, Poradní výbor k Úmluvě č. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu]*, T-PD(2017)01, Štrasburk, 23. ledna 2017.

založeného na algoritmech, které mohou zajistit nebývalé pronikání do lidského chování a soukromého života.[976]

Nové technologie jsou účinné a mohou být mimořádně nebezpečné, pokud se dostanou do nesprávných rukou. Státní orgány provádějící činnosti hromadného dohledu, které mohou těchto technologií využívat, jsou jedním z příkladů významného dopadu, který tyto technologie mohou mít na práva jednotlivců. Odhalení učiněná Edwardem Snowdenem v roce 2013 o provozování programů rozsáhlého sledování internetu a telefonní komunikace ze strany zpravodajských služeb v některých státech vyvolala značné obavy ohledně nebezpečí, které činnosti sledování představují pro soukromí, demokratickou správu a svobodu projevu. Hromadné sledování a technologie umožňující globalizované ukládání a zpracovávání osobních informací a hromadný přístup k údajům mohou být v rozporu se samotnou podstatou práva na soukromí.[977] Kromě toho mají negativní dopad na politickou kulturu a jsou překážkou demokracie, kreativity a inovací.[978] Už jen pouhý strach, že stát může soustavně sledovat a analyzovat chování a jednání občanů, je může odrazovat od vyjadřování názorů na určité záležitosti, což může mít za následek opatrnost a obezřetnost.[979] Tyto výzvy přiměly řadu veřejných orgánů, výzkumných středisek a organizací občanské společnosti, aby analyzovaly možné dopady nových technologií na společnost. V roce 2015 evropský inspektor ochrany údajů zahájil několik iniciativ, které měly posoudit dopad dat velkého objemu a internetu věcí na etiku. Zejména pak zřídil etickou poradní skupinu, která si klade za cíl stimulovat „otevřenou a informovanou diskusi o digitální etice, která umožní, aby si EU uvědomila výhody technologií pro společnost i hospodářství, a která současně posílí práva a svobody jednotlivců, zejména jejich práva na soukromí a ochranu údajů".[980]

Zpracování osobních údajů je také mocný nástroj v rukou korporací. V dnešní době může odhalit podrobné informace o zdravotním či finančním stavu dané osoby.

976 Evropský parlament (2017), Usnesení o dopadech dat velkého objemu na základní práva: soukromí, ochrana údajů, zákaz diskriminace, bezpečnost a prosazování práva (P8_TA-PROV(2017)0076, Štrasburk, 14. března 2017.

977 Viz OSN, Valné shromáždění, *Zpráva zvláštního zpravodaje o prosazování a ochraně lidských práv a základních svobod při boji proti terorismu*, Ben Emmerson, A/69/397, 23. září 2014, bod 59. Viz také ESLP, *Informativní přehled o hromadném sledování*, červenec 2017.

978 EIOÚ (2015), *Meeting the challenges of big data [Jak obstát ve výzvě, jíž představují data velkého objemu]*, stanovisko 7/2015, Brusel, 19. listopadu 2015.

979 Viz zejména rozsudek SDEU (velkého senátu) ze dne 8. dubna 2014, spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, bod 37.

980 EIOÚ, Rozhodnutí ze dne 3. prosince 2015, kterým se zřizuje externí poradní skupina k etickým aspektům ochrany údajů („etická poradní skupina"), 3. prosince 2015, 5. bod odůvodnění.

Tyto informace pak mohou použít korporace k tomu, aby učinily rozhodnutí důležitá pro jednotlivce, například výši pojistného u zdravotního pojištění, kterou budou platit, nebo jejich úvěruschopnost. Techniky zpracování údajů mohou mít vliv i na demokratické procesy, pokud je použijí politici nebo korporace k ovlivnění voleb – například prostřednictvím „mikrocílení" komunikace voličů. Jinými slovy, zatímco soukromí bylo původně považováno za právo na ochranu jednotlivců před neodůvodněnými zásahy ze strany orgánů veřejné moci, v moderní době může být ohrožováno i soukromými aktéry. To vyvolává otázky ohledně používání technologie a prediktivní analýzy při rozhodování, které ovlivňuje každodenní život jednotlivců, a zdůrazňuje nutnost zajistit, aby veškeré zpracování osobních údajů bylo v souladu s požadavky na dodržování základních práv.

Ochrana údajů je nerozlučně spjata s technologickými, sociálními a politickými změnami. Proto je nemožné sestavit vyčerpávající seznam budoucích výzev. V této kapitole zkoumáme vybrané oblasti týkající se dat velkého objemu, internetových sociálních sítí a jednotného digitálního trhu EU. Nejedná se o vyčerpávající zhodnocení těchto oblastí z hlediska ochrany údajů, nýbrž se zde upozorňuje na řadu možných interakcí mezi novými nebo revidovanými lidskými činnostmi a ochranou údajů.

10.1. Data velkého objemu, algoritmy a umělá inteligence

Hlavní body

- Přelomové inovace v oblasti IKT utvářejí nový způsob života, v němž jsou sociální vztahy, podnikání, soukromé a veřejné služby navzájem digitálně propojené, čímž se vytváří stále větší objem údajů, z nichž řada představuje osobní údaje.
- Vlády, podniky a občané se stále častěji zapojují do ekonomiky založené na datech, ve které se data jako taková stala hodnotnými aktivy.
- Pojem data velkého objemu označuje jak tato data, tak jejich analýzu.
- Osobní údaje zpracovávané prostřednictvím analýzy dat velkého objemu spadají do působnosti právních předpisů EU a RE.
- Odchylky od pravidel a práv v oblasti ochrany údajů jsou omezeny na vybraná práva a na zvláštní situace, za kterých by se vynucování určitého práva ukázalo jako nemožné nebo by vyžadovalo nepřiměřené úsilí ze strany správců údajů.

- Plně automatizované rozhodování je obecně zakázáno, s výjimkou konkrétních případů.
- Povědomí u jednotlivců a kontrola z jejich strany jsou klíčem k zajištění vynucování práv.

V našem stále více digitálním světě zanechává každá činnost digitální stopu, kterou je možné shromažďovat, zpracovávat a vyhodnocovat nebo analyzovat. Novými informačními a komunikačními technologiemi se shromažďuje a zaznamenává stále více údajů.[981] Až donedávna nebyla žádná technologie schopna analyzovat či hodnotit velký objem údajů nebo vyvodit užitečné závěry. Dat bylo jednoduše příliš mnoho, aby je bylo možné vyhodnocovat, a byla příliš složitá, špatně organizovaná a proměnlivá, aby bylo možné určit trendy a návyky.

10.1.1. Definice dat velkého objemu, algoritmů a umělé inteligence

Data velkého objemu

Pojem „data velkého objemu" může označovat několik koncepcí, a to v závislosti na kontextu. Běžně zahrnuje „rostoucí schopnost technologií shromažďovat, zpracovávat a těžit nové a prediktivní poznatky z velkého objemu rychlých a rozmanitých dat".[982] Pojem data velkého objemu tedy označuje jak tato data jako taková, tak jejich analýzu.

Data pochází z různých druhů **zdrojů** a zahrnují osoby a jejich osobní údaje, stroje nebo senzory, informace o klimatu, družicové snímkování, digitální fotografie a videa nebo signály GPS. Mnoho těchto dat a informací jsou však osobní údaje – počínaje jménem, fotografií, e-mailovou adresou a bankovními údaji přes data sledování

981 Evropská komise, Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Na cestě k prosperující ekonomice založené na datech", COM(2014) 442 final, Brusel, 2. července 2014.

982 Rada Evropy, Poradní výbor k Úmluvě č. 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 2; Evropská komise, Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Na cestě k prosperující ekonomice založené na datech", COM(2014) 442 final, Brusel, 2. července 2014, na s. 4; Mezinárodní telekomunikační unie (2015), Doporučení Y.3600. Data velkého objemu – požadavky a schopnosti založené na cloud computingu.

pomocí GPS a příspěvky na webových stránkách sociálních sítí až po lékařské informace a IP adresu počítače.[983]

Daty velkého objemu se také rozumí **zpracování**, analýza a vyhodnocení velkého objemu dat a dostupných informací, tj. s cílem získat užitečné informace pro účely analýzy dat velkého objemu. To znamená, že shromážděná data a informace mohou být použity pro jiné účely, než pro které byly původně zamýšleny, např. statistické trendy nebo služby více uzpůsobené na míru, jako je reklama. Ve skutečnosti pak, pokud existují technologie na shromažďování, zpracování a vyhodnocování dat velkého objemu, jakýkoliv druh informací je možné kombinovat a opětovně hodnotit: finanční transakce, úvěruschopnost, lékařské ošetření, soukromá spotřeba, profesní činnost, sledování a zvolené trasy, používání internetu, elektronických karet a chytrých telefonů, sledování videa nebo komunikace. Analýza dat velkého objemu přináší nový kvantitativní rozměr dat, který je možné vyhodnocovat a používat v reálném čase, například za účelem poskytování služeb uzpůsobených na míru spotřebitelům.

Algoritmy a umělá inteligence

Umělou inteligencí (UI) se rozumí inteligence strojů, které jednají jako „inteligentní aktéři". Jako inteligentní aktér mohou některé přístroje za pomoci softwaru vnímat své okolí a přijímat opatření podle algoritmů. Pojem UI se používá tehdy, pokud stroj napodobuje „kognitivní" funkce – jako je učení a řešení problémů –, které by obvykle byly spojeny s fyzickými osobami.[984] K napodobování procesu rozhodování používají moderní technologie a software algoritmy, které přístroje používají k „automatizovaným rozhodnutím". Algoritmus lze nejlépe popsat jako postup výpočtu, zpracování údajů, vyhodnocování a automatizovaného uvažování a rozhodování krok za krokem.

Obdobně jako v případě analýzy dat velkého objemu vyžaduje UI a automatizované rozhodování, které vytváří, kompilaci a zpracování velkých objemů dat. Tato data mohou pocházet z přístroje samotného (teplota brzd, palivo atd.) nebo z okolního

983 Evropská komise, Fact Sheet on The EU Data Protection Reform and Big Data [Informativní přehled o reformě ochrany údajů v EU a o datech velkého objemu]; Rada Evropy, Poradní výbor k Úmluvě č. 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 2.

984 Stuart Russel a Peter Norvig, *Artificial Intelligence: A Modern Approach [Umělá inteligence: moderní přístup] (2. vydání)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, s. 27, 32–58, 968–972; Stuart Russel a Peter Norvig, *Artificial Intelligence: A Modern Approach [Umělá inteligence: moderní přístup] (3. vydání)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

prostředí. Například profilování je proces, který může spoléhat na automatizované rozhodování podle předem nastavených vzorců nebo faktorů.

Příklad: Profilování a cílená reklama

Profilování založené na datech velkého objemu zahrnuje hledání souvislostí, které odrážejí „charakteristiku typu osobnosti" – například pokud společnosti působící v oblasti nakupování on-line navrhují produkty, které „by se vám také mohly líbit" na základě získaných informací o tom, jaké produkty byly v minulosti umístěny do nákupního košíku zákazníka. Čím více údajů, tím jasnější je mozaika. Například chytrý telefon je účinný dotazník, který jednotlivci vyplňují každým použitím, ať už vědomě, či nikoliv.

Moderní psychografie – věda o studiu osobností – používá metodu OCEAN, na jejímž základě určuje typy charakteru dané osoby. „Velká pětka" charakterových vlastností se týká otevřenosti (jak otevřená je daná osoba novinkám), svědomitosti (jak blízko je daná osoba perfekcionismu), extraverze (jak je daná osoba společenská), přívětivosti (jak je daná osoba přívětivá) a neuroticismu (jak je daná osoba zranitelná). Na základě těchto informací se vytváří profily dané osoby, jejích potřeb a obav, jak se bude chovat atd. Tento profil je následně doplněn o jiné informace o dané osobě získané z veškerých dostupných zdrojů, od obchodníků s údaji, ze sociálních sítí (včetně „lajků" u příspěvků a zveřejněných fotografií), z toho, jakou hudbu daná osoba poslouchá on-line, nebo údajů z GPS a sledování.

Velký počet profilů, které byly vytvořeny prostřednictvím technik analýzy dat velkého objemu, se následně porovnává s cílem určit podobnosti chování a sestavit klastry osobností. Informace o chování a postojích některých osobností jsou tudíž invertovány. S přístupem k datům velkého objemu a jejich použitím se test osobnosti obrátil. Informace o chování a postojích se nyní používají k popisu osobnosti jednotlivce. Pokud máme kombinací informací o „lajcích" na sociálních sítích, údajů o sledování, o hudbě, kterou daná osoba poslouchá, a filmech, které zhlíží, můžeme získat jasný obraz o osobnosti daného jednotlivce, což podnikům umožňuje předávat na míru uzpůsobenou reklamu a/nebo informace podle „osobnosti" daného člověka. Především však tyto informace mohou být zpracovány v reálném čase.[985]

985 Techniky zpracovávání a nový software hodnotí informace o tom, co se dané osobě líbí, na co se dívá při nakupování on-line nebo co vkládá do on-line nákupního košíku v reálném čase, a mohou navrhovat „produkty", které mohou být zajímavé vzhledem ke shromážděným informacím.

10.1.2. Hledání rovnováhy mezi přínosy a riziky dat velkého objemu

Moderní techniky zpracování mohou zpracovávat velké objemy dat, rychle vkládat nová data, zajišťovat zpracování informací v reálném čase, pokud jde o krátkou dobu reakce (dokonce i v případě složitých žádostí), zajišťovat možnost vícečetných a současných žádostí, a mohou analyzovat různé druhy informací (fotografie, texty nebo čísla). Tyto technologické inovace umožňují strukturovat, zpracovávat a hodnotit velké objemy dat a informací v reálném čase.[986] Exponenciálním navýšením objemu dostupných a analyzovaných dat je možné dosáhnout výsledků, které by nebyly možné v analýze menšího rozsahu. Data velkého objemu přispěla ke vzniku nového odvětví podnikání, ve kterém mohou pro podniky i spotřebitele vznikat nové služby. Hodnota osobních údajů občanů EU má potenciál vzrůst každoročně do roku 2020 o téměř 1 bilion EUR.[987] Proto mohou data velkého objemu nabídnout nové **příležitosti** vyplývající z hodnocení velkého množství dat za účelem vyvození nových sociálních, ekonomických či vědeckých závěrů, které mohou být ku prospěchu jednotlivcům, ale i podnikům a vládám.[988]

Analýza dat velkého objemu může odhalit souvislosti mezi různými zdroji a soubory údajů, čímž umožní získat užitečný vhled v oblastech, jako je věda a medicína. Tak je tomu například v oblastech, jako je zdravotnictví, potravinové zabezpečení, inteligentní systémy dopravy, energetická účinnost nebo městské plánování. Tato analýza informací v reálném čase může být použita k vylepšení prováděných

986 Vývoj softwaru pro zpracování dat velkého objemu je stále v rané fázi. Přesto byly nedávno vyvinuty analytické programy, zejména pro analýzu velkého objemu dat a informací v reálném čase, které se týkají činností jednotlivců. Možnost analýzy a zpracování dat velkého objemu strukturovaným způsobem nabízí nové prostředky profilování a cílené reklamy. Evropská komise, Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Na cestě k prosperující ekonomice založené na datech COM(2014) 442 final, Brusel, 2. července 2014; Evropská komise, Fact Sheet on The EU Data Protection Reform and Big Data [Informativní přehled o reformě ochrany údajů v EU a o datech velkého objemu] a Rada Evropy, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 2.

987 Evropská komise, Fact Sheet on EU Data Protection Reform and Big Data [Informativní přehled o reformě ochrany údajů v EU a o datech velkého objemu].

988 Mezinárodní konference komisařů pro ochranu údajů (2014), Usnesení o datech velkého objemu a Evropská komise, Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Na cestě k prosperující ekonomice založené na datech COM(2014) 442 final, Brusel, 2. července 2014, na s. 2; Evropská komise, Fact Sheet on The EU Data Protection Reform and Big Data [Informativní přehled o reformě ochrany údajů v EU a o datech velkého objemu] a Rada Evropy, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 1.

systémů. Ve výzkumu je možné získat nové informace kombinováním dat velkého objemu a statistických hodnocení, zejména v oborech, ve kterých bylo až dosud mnoho údajů vyhodnocováno pouze manuálně. Je možné vyvinout nové postupy léčby, které budou upraveny na míru pacientům, a to na základě porovnání s dostupným velkým objemem informací. Podniky doufají, že jim analýza dat velkého objemu umožní získat konkurenční výhodu, vytvoří potenciální úspory a dá vzniknout novým oblastem podnikání prostřednictvím přímých, individualizovaných zákaznických služeb. Vládní agentury doufají, že dosáhnou zlepšení v oblasti trestního soudnictví. Strategie pro jednotný digitální trh v Evropě, kterou předložila Komise, uznává potenciál technologií a služeb založených na datech a dat velkého objemu, které se mohou stát katalyzátorem hospodářského růstu, inovací a digitalizace v EU.[989]

Data velkého objemu však rovněž obnášejí **rizika**, obecně spojená s atributy „tří V": objem (volume), rychlost (velocity) a rozmanitost (variety) zpracovávaných dat. Objemem se rozumí objem zpracovávaných dat, rozmanitostí počet a rozmanitost druhů dat, zatímco rychlost označuje rychlost zpracování dat. Zvláštní otázky týkající se ochrany údajů vyvstávají zejména tehdy, pokud je analýza dat velkého objemu použita na velkých souborech dat s cílem vytěžit nové a prediktivní znalosti pro účely rozhodování týkající se jednotlivců a/nebo skupin.[990] Rizika pro ochranu údajů a soukromí týkající se dat velkého objemu byla zdůrazněna ve stanoviscích EIOÚ a pracovní skupiny zřízené podle článku 29, v usneseních Evropského parlamentu a v politických dokumentech Rady Evropy.[991]

K rizikům může patřit neoprávněné zacházení s daty velkého objemu ze strany osob s přístupem k velkému objemu informací prostřednictvím manipulace, diskriminace nebo útisku jednotlivců nebo zvláštních skupin ve společnosti.[992] Pokud se shromaž-

989 Usnesení Evropského parlamentu ze dne 14. března 2017 o dopadech dat velkého objemu na základní práva: soukromí, ochrana údajů, zákaz diskriminace, bezpečnost a prosazování práva (2016/2225(INI)).

990 Rada Evropy, Poradní výbor podle Úmluvy č. 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 2.

991 Viz například EIOÚ (2015), *Meeting the Challenges of big data [Jak obstát ve výzvě, již představují data velkého objemu]*, stanovisko 7/2015, 19. listopadu 2015; EIOÚ (2016), *Coherent enforcement of fundamental rights in the age of Big Data [Soudržné prosazování základních práv v éře dat velkého objemu]*, stanovisko 8/2016, 23. září 2016; Evropský parlament (2016), Usnesení Evropského parlamentu o dopadech dat velkého objemu na základní práva: soukromí, ochrana údajů, zákaz diskriminace, bezpečnost a prosazování práva, P8_TA(2017)0076, Štrasburk, 14. března 2017; Rada Evropy, Poradní výbor podle Úmluvy č. 108, Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu, T-PD(2017)01, Štrasburk, 23. ledna 2017.

992 Mezinárodní konference komisařů pro ochranu údajů (2014), Usnesení o datech velkého objemu.

dují, zpracovávají a vyhodnocují velké objemy osobních údajů či informací o chování jednotlivců, může jejich neoprávněné využití vést k významnému porušení základních práv a svobod, které dalece překračují právo na soukromí. Přesné měření rozsahu, v němž může být dotčeno soukromí a osobní údaje, není možné. Evropský parlament konstatoval, že chybí metodika k posouzení celkového dopadu dat velkého objemu na základě důkazů, ale existují důkazy svědčící o tom, že analýzy dat velkého objemu mohou mít významný horizontální dopad na veřejný i soukromý sektor.[993]

Obecné nařízení o ochraně osobních údajů obsahuje ustanovení o právu nebýt předmětem automatizovaného rozhodování, včetně profilování.[994] Otázka soukromí vyvstane, pokud výkon práva vznést námitku vyžaduje lidský zásah, což subjektům údajů umožňuje vyjádřit jejich názor a napadnout rozhodnutí.[995] Na základě toho se mohou objevit výzvy při zajišťování dostatečné úrovně ochrany osobních dat, například pokud není možný žádný lidský zásah nebo pokud algoritmy jsou příliš složité a objem příslušných dat příliš velký na to, aby bylo jednotlivcům možné poskytnout odůvodnění některých rozhodnutí a/nebo je informovat předem za účelem získání jejich souhlasu. Příklad použití UI a automatizovaného rozhodování lze nalézt v nedávném vývoji v oblasti žádostí o hypotéku nebo během procesů náboru. Žádosti byly zamítnuty nebo odmítnuty na základě skutečnosti, že žadatelé nesplňují předem stanovené parametry nebo faktory.

10.1.3. Otázky související s ochranou údajů

Z hlediska ochrany údajů se hlavní otázky týkají na jedné straně objemu a rozmanitosti zpracovávaných osobních údajů a na straně druhé zpracování a jeho důsledků. Zavedení složitých algoritmů a softwaru pro přeměnu velkých objemů dat do podoby zdroje pro účely rozhodování ovlivňuje jednotlivce a zejména skupiny, především pak v případech profilování nebo nálepkování, a tím v konečném důsledku vyvolává řadu otázek týkajících se ochrany údajů.[996]

993 Usnesení Evropského parlamentu ze dne 14. března 2017 o dopadech dat velkého objemu na základní práva: soukromí, ochrana údajů, zákaz diskriminace, bezpečnost a prosazování práva (2016/2225(INI)).

994 Obecné nařízení o ochraně osobních údajů, článek 22.

995 Tamtéž, čl. 22 odst. 3.

996 Rada Evropy, Poradní výbor podle Úmluvy č. 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu], 23. ledna 2017, na s. 2.

Identifikace správců a zpracovatelů a jejich odpovědnost

Data velkého objemu a UI vyvolávají několik otázek v souvislosti s identifikací správců a zpracovatelů a jejich odpovědností: pokud se shromáždí a zpracovává takovýto velký objem údajů, kdo je jejich majitelem? Pokud údaje zpracovávají inteligentní stroje a software, kdo je správcem? Jaké má přesně každý subjekt v rámci zpracování povinnosti? A za jakými účely je možné data velkého objemu používat?

Otázka odpovědnosti v souvislosti s UI se stane o to složitější, pokud UI přijímá rozhodnutí založená na zpracování dat, které sama vyvinula. Obecné nařízení o ochraně osobních údajů stanoví právní rámec pro odpovědnost správce a zpracovatele údajů. Nezákonné zpracování osobních údajů zakládá odpovědnost správce a zpracovatele údajů.[997] Umělá inteligence a automatizované rozhodování vyvolávají otázky, kdo je zodpovědný za porušení předpisů, které bude mít dopad na soukromí subjektů údajů, pokud nelze s jistotou stanovit složitost a objem zpracovávaných údajů. Pokud se UI a algoritmy považují za produkty, vyvstávají otázky ohledně hranice mezi osobní odpovědností, která je upravena obecným nařízením o ochraně osobních údajů, a odpovědností produktu, která tímto nařízením upravena není.[998] Za tímto účelem by bylo třeba pravidel týkajících se odpovědnosti s cílem zaplnit mezeru mezi osobní odpovědností a odpovědností produktu za robotiku a UI, například včetně automatizovaného rozhodování.[999]

Dopad na zásady ochrany údajů

Povaha, analýza a použití dat velkého objemu popsané výše představuje výzvu pro použití některých tradičních, základních zásad evropského práva v oblasti ochrany údajů.[1000] Tyto výzvy se především týkají zásady zákonnosti, minimalizace údajů, účelového omezení a transparentnosti.

Zásada minimalizace údajů vyžaduje, aby byly osobní údaje přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány.

997 Obecné nařízení o ochraně osobních údajů, články 77 až 79 a článek 82.

998 Evropský parlament, Evropská občanskoprávní pravidla pro robotiku, generální ředitelství pro vnitřní politiky, (říjen 2016), s. 14.

999 Projev Roberta Violy na mediálním semináři týkajícím se evropských pravidel pro robotiku v Evropském parlamentu. (PROJEV ze dne 16. února 2017); oznámení Evropského parlamentu týkající se žádosti o návrh pravidel občanskoprávní odpovědnosti pro robotiku a UI určené Komisi.

1000 Rada Evropy, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu]*, T-PD(2017)01, Štrasburk, 23. ledna 2017.

Avšak obchodní model dat velkého objemu může být antitezí minimalizace údajů, protože vyžaduje stále více údajů, často pro nespecifikované účely.

Totéž platí i u zásady účelového omezení, která vyžaduje, aby údaje byly zpracovávány pro konkrétní účely a aby nebyly používány pro účely, které jsou neslučitelné s původním účelem shromažďování, ledaže toto zpracování vychází ze zákonného důvodu – například (ale nikoliv výlučně) souhlasu subjektu údajů (viz oddíl 4.1.1).

Data velkého objemu v neposlední řadě rovněž zpochybňují zásadu přesnosti údajů, protože aplikace zpracovávající data velkého objemu často shromažďují údaje z různých zdrojů, aniž by existovala možnost kontroly a/nebo zachování přesnosti shromážděných údajů.[1001]

Zvláštní pravidla a práva

I nadále platí obecné pravidlo, že osobní údaje zpracovávané prostřednictvím analýzy dat velkého objemu spadají do působnosti právních předpisů v oblasti ochrany údajů. Do práva EU a RE však byla zavedena zvláštní pravidla či odchylky pro konkrétní případy v souvislosti s algoritmickým složitým zpracováním údajů.

V rámci práva RE přiznává Modernizovaná úmluva č. 108 nová práva subjektu údajů s cílem umožnit účinnější kontrolu jeho osobních údajů ve věku rozmachu dat velkého objemu. Přesně tak je tomu například v případě čl. 9 odst. 1 písm. a), c) a d) Modernizované úmluvy týkajícím se práva nebýt předmětem rozhodnutí, které danou osobu významně ovlivňuje, pouze na základě automatizovaného zpracování údajů, aniž by bylo přihlédnuto k názorům dané osoby; práva získat na požádání informace o důvodech, na nichž je založeno zpracování údajů, jehož výsledky se uplatní na danou osobu, jakož i práva vznést námitku. Další ustanovení Modernizované úmluvy č. 108, zejména povinnost transparentnosti a další povinnosti, jsou doplňkové prvky ochranného mechanismu stanoveného v Modernizované úmluvě č. 108 s cílem bojovat proti digitálním výzvám.

V právu EU, kromě případů uvedených v článku 23 GDPR, musí být zajištěna **transparentnost** veškerého zpracování osobních údajů. To je zvlášť důležité v souvislosti s internetovými službami a jiným složitým automatizovaným zpracováním údajů, jako je použití algoritmů pro rozhodování. V tomto případě musí prvky systémů pro

1001 EIOÚ (2016), *Coherent enforcement of fundamental rights in the age of Big Data [Soudržné prosazování základních práv v éře dat velkého objemu]*, stanovisko 8/2016, 23. září 2016, s. 8.

zpracování údajů subjektům údajů umožňovat, aby skutečně porozuměly tomu, co se děje s jejich údaji. K zajištění korektního a transparentního zpracování ukládá obecné nařízení o ochraně osobních údajů správci povinnost poskytnout subjektu údajů smysluplné informace týkající se logiky automatizovaného zpracování, včetně profilování.[1002] Ve svém doporučení o ochraně a podpoře práva na svobodu projevu a práva na soukromý život vzhledem k neutralitě sítě doporučil Výbor ministrů Rady Evropy, aby poskytovatelé internetových služeb „poskytli uživatelům jasné, úplné a veřejně dostupné informace, pokud jde o veškeré postupy řízení provozu, které mohou ovlivnit přístup uživatelů k obsahu, aplikacím či službám a jejich distribuci".[1003] Zprávy o praktikách v oblasti řízení internetového provozu, sestavené příslušnými orgány ve všech členských státech, by měly být vypracovány otevřeně a transparentně a měly by být zpřístupněny veřejnosti zdarma.[1004]

Správci údajů musí **informovat** subjekty údajů **–** ať už o tom, kdy od nich shromažďují údaje, nebo kdy od nich údaje shromažďovány nebyly – nejen o konkrétních informacích o shromažďovaných údajích a zamýšleném zpracování (viz oddíl 6.1.1), ale také v relevantních případech o existenci procesů automatizovaného rozhodování a poskytnout jim „smysluplné informace týkající se použitého postupu"[1005], cílů a možných důsledků těchto postupů. Obecné nařízení o ochraně osobních údajů rovněž objasňuje (nejen v případech, kdy osobní údaje nebyly získány od subjektu údajů), že správce není povinen poskytnout subjektu údajů tyto informace, pokud „poskytnutí těchto informací není možné nebo by vyžadovalo neúměrné úsilí".[1006] Jak však zdůraznila pracovní skupina zřízená podle článku 29 ve svých *Pokynech k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, složitost zpracování by sama o sobě neměla zbavovat správce údajů povinnosti poskytovat subjektu údajů jasné vysvětlení cílů a analýzy použité v rámci zpracování údajů.[1007]

Práva subjektů údaj na **přístup**, **opravu** a **výmaz** jejich osobních údajů, jakož i jejich právo na **omezení** zpracování nezahrnují podobnou výjimku. Avšak od povinnosti

1002 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. f).

1003 Rada Evropy, Výbor ministrů (2016), Doporučení Výboru ministrů členským státům CM/Rec(2016)1 o ochraně a podpoře práva na svobodu projevu a práva na soukromý život vzhledem k neutralitě sítě, 13. ledna 2016, bod 5.1.

1004 Tamtéž, bod 5.2.

1005 Obecné nařízení o ochraně osobních údajů, čl. 13 odst. 2 písm. f) a čl. 14 odst. 2 písm. g).

1006 Tamtéž, čl. 14 odst. 5 písm. b).

1007 Pracovní skupina zřízená podle článku 29, *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, WP 251, 3. října 2017, s. 14.

správce údajů oznámit subjektu údajů veškeré opravy nebo výmaz jejich osobních údajů (viz oddíl 6.1.4) může být rovněž upuštěno, pokud by toto oznámení nebylo „možné nebo by vyžadovalo neúměrné úsilí“.[1008]

Subjekty údajů mají rovněž právo **vznést námitku** v souladu s článkem 21 GDPR (viz oddíl 6.1.6) vůči veškerému zpracování svých osobních údajů, včetně případů analýzy dat velkého objemu. Ačkoliv správci údajů mohou být osvobozeni od této povinnosti, pokud mohou prokázat převažující oprávněné zájmy, nemohou této výjimky pro zpracování využít pro účely přímého marketingu.

Zvláštní odchylky od tohoto práva mohou též uplatnit správci údajů, pokud zpracovávají osobní údaje pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[1009]

V souvislosti s **profilováním a automatizovaným rozhodováním** zavedlo GDPR zvláštní pravidla: Článek 22 odst. 1 stanoví, že subjekt údajů „má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, které má pro něho právní účinky“. Jak je zdůrazněno v pokynech pracovní skupiny zřízené podle článku 29, uvádí tento článek obecný zákaz plně automatizovaného rozhodování.[1010] Správci údajů mohou být od tohoto zákazu osvobozeni pouze ve třech zvláštních případech: pokud je rozhodnutí: 1) nezbytné k plnění smlouvy mezi subjektem údajů a správcem, 2) povoleno právem Unie nebo členského státu nebo 3) založeno na výslovném souhlasu.[1011]

Individuální kontrola

Složitost a nedostatečná transparentnost analýzy dat velkého objemu může vyžadovat přehodnocení koncepce individuální kontroly osobních údajů. Měla by být upravena na míru danému sociálnímu a technologickému kontextu a zohledňovat nedostatečné znalosti na straně jednotlivců. Ochrana údajů v oblasti dat velkého objemu by proto měla přijmout širší koncepci kontroly používání údajů, podle které

1008 Obecné nařízení o ochraně osobních údajů, článek 19.

1009 Tamtéž, čl. 89 odst. 2 a 3.

1010 Pracovní skupina zřízená podle článku 29, *Pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679*, WP 251, 3. října 2017, s. 9.

1011 Obecné nařízení o ochraně osobních údajů, čl. 22 odst. 2.

se individuální kontrola vyvíjí do podoby složitějšího procesu vypracování více posouzení dopadu rizik spojených s používáním údajů.[1012]

Kvalita aplikace zpracovávající data velkého objemu závisí na tom, jak dobře umí předvídat touhy nebo chování zkušebních jednotlivců (nebo spotřebitelů). Současné modely predikce založené na analýze dat velkého objemu se soustavně zpřesňují. Současný vývoj zahrnuje nejen používání dat za účelem kategorizace osobností (tj. chování a postojů), ale analyzuje chování pomocí analýzy vzorců hlasu a intenzity zadávání zpráv nebo prostřednictvím tělesné teploty. Všechny tyto informace mohou být použity v reálném čase s ohledem na znalosti čerpané z vyhodnocování dat velkého objemu za účelem posouzení úvěruschopnosti například během schůze se zástupcem banky. Hodnocení se neprovádí na základě dosažených výsledků jednotlivce, který o úvěr žádá, ale na základě behaviorálních charakteristik získaných z analýzy a vyhodnocování informací z dat velkého objemu, tj. zda uchazeč mluví rozhodným nebo lichotivým hlasem, jaká je jeho řeč těla nebo tělesná teplota.

Profilování a cílená reklama nemusejí být nevyhnutelně problémem, pokud si jednotlivci jsou **vědomi**, že jsou předmětem cílené reklamy. Profilování se stává problémem, pokud se použije k manipulaci jednotlivci, tj. k vyhledávání určitých osobností nebo skupin lidí za účelem vedení politické kampaně. Například na skupinu nerozhodnutých voličů je možné cílit politickými sděleními uzpůsobenými na míru jejich „osobnosti" a postojům. Jiným problémem by mohlo být použití tohoto profilování k odepření přístupu k výrobkům a službách některým jednotlivcům. Jednou ze záruk, které mohou být použity na ochranu před takovýmto zneužíváním dat velkého objemu a osobních informací, je pseudonymizace (viz oddíl 2.1.1).[1013] Pokud jsou osobní údaje skutečně anonymizovány, tj. neexistují informace, které by zanechávaly stopy, které by je spojovaly se subjektem údajů, spadají tyto případy mimo oblast působnosti obecného nařízení o ochraně osobních údajů. Souhlas subjektů údajů a jednotlivců se zpracováním dat velkého objemu představuje také výzvu pro právo v oblasti ochrany údajů. Patří sem souhlas s tím, že jednotlivec bude předmětem na míru uzpůsobené reklamy a profilování, které může být odůvodněno „zlepšením zážitku zákazníků", a souhlas s použitím velkých objemů osobních údajů za účelem zpřesnění a vývoje analytických nástrojů založených na informacích. Povědomí (nebo jeho absence) o zpracování dat velkého objemu vyvolává několik otázek týkajících se prostředků, jimiž mohou subjekty údajů uplatňovat svá práva, protože

1012 Rada Evropy, Poradní výbor k Úmluvě č. 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data [Pokyny týkající se ochrany jednotlivců s ohledem na zpracování osobních údajů ve světě dat velkého objemu]*, T-PD(2017)01, Štrasburk, 23. ledna 2017.

1013 Tamtéž, s. 2.

zpracování dat velkého objemu může vycházet jak z pseudonymizovaných, tak z anonymizovaných informací, které se řídí algoritmy. Zatímco pseudonymizované údaje spadají do působnosti obecného nařízení o ochraně osobních údajů, na anonymizované údaje se nařízení nepoužije. Kontrola a povědomí o zpracování osobních údajů ze strany jednotlivců jsou klíčové pro analýzu dat velkého objemu: bez nich nebudou mít jasnou představu o tom, kdo je správcem nebo zpracovatelem údajů, což jim zabrání v účinném výkonu jejich práv.

10.2. Web 2.0 a 3.0: sociální sítě a internet věcí

Hlavní body

- Sociální sítě jsou on-line komunikační platformy, které umožňují jednotlivcům připojit se k sítím podobně smýšlejících uživatelů nebo tyto sítě vytvářet.
- Internet věcí je připojení objektů k internetu a propojení objektů mezi sebou navzájem.
- Souhlas subjektů údajů je nejčastějším právním základem pro zákonné zpracování údajů ze strany správců údajů na sociálních sítích.
- Uživatelé sociálních sítí jsou obecně chráněni „výjimkou pro domácnosti“, tato výjimka však může být za určitých podmínek zrušena.
- Poskytovatelé sociálních sítí „výjimkou pro domácnosti“ chráněni nejsou.
- K zajištění bezpečnosti údajů v tomto oboru je nezbytná záměrná a standardní ochrana soukromí.

10.2.1. Definice webu 2.0 a 3.0

Sociální sítě

Původně byl internet koncipován jako síť pro propojení počítačů a předávání zpráv. Možnosti výměny dat byly omezené, webové stránky nabízely pouze možnost, aby si jednotlivci pasivně prohlíželi jejich obsah.[1014] V éře webu 2.0 se internet změnil do podoby fóra, kde uživatelé interagují, spolupracují a vytvářejí příspěvky. Pro tuto éru je typický pozoruhodný úspěch a rozšířené používání sociálních sítí, které jsou nyní nedílnou součástí každodenního života milionů lidí.

1014 Evropská komise (2016), *Advancing the Internet of Things in Europe [Dosahování pokroku v oblasti internetu věcí v Evropě]*, SWD(2016) 110 final.

Sociální sítě nebo „sociální média" mohou být široce definovány jako „on-line komunikační platformy, které jednotlivcům umožňují připojit se k sítím nebo vytvářet sítě stejně smýšlejících uživatelů".[1015] Aby se mohli jednotlivci připojit k síti nebo ji vytvořit, jsou vyzváni, aby poskytli své osobní údaje a vytvořili si profil. Sociální sítě umožňují uživatelům vytvořit digitální „obsah", který zahrnuje vše počínaje fotografiemi a videi až po odkazy na novinové články a osobní příspěvky vyjadřující názory těchto jednotlivců. Prostřednictvím těchto platforem on-line komunikace mohou uživatelé interagovat a komunikovat s několika dalšími uživateli. Především pak většina oblíbených sociálních sítí nevyžaduje žádné registrační poplatky. Místo aby nutili uživatele platit za připojení k síti, získávají poskytovatelé sociálních sítí většinu svého příjmu z cílené reklamy. Inzerenti mohou mít velký prospěch z osobních informací, které jsou na těchto stránkách odhalovány každý den. To, že disponují informacemi o věku, pohlaví, místě a zájmech uživatelů, jim umožňuje oslovit reklamou ty „pravé" lidi.

Výbor ministrů Rady Evropy přijal doporučení o ochraně lidských práv na sociálních sítích,[1016] které se ve zvláštním oddílu zabývá ochranou údajů a které bylo v roce 2018 doplněno jiným doporučením o úloze a odpovědnosti internetových zprostředkovatelů.[1017]

Příklad: Nora má velkou radost, protože ji její partner požádal o ruku. Chce se o tuto dobrou zprávu podělit s přáteli a rodinou a rozhodne se napsat příspěvek naplněný emocemi na sociální síť, ve kterém svou radost vyjádří, a také se rozhodne změnit svůj rodinný stav na „zasnoubená". Když se v dalších dnech Nora přihlásí ke svému účtu, vidí reklamy na svatební šaty a květinářství. Proč?

Při vytváření reklamy na Facebooku zvolily společnosti prodávající svatební šaty a květiny určité parametry, aby mohly oslovit lidi, jako je Nora. Když ukazatele na Nořině profilu oznamují, že je žena, zasnoubená, žije v Paříži, blízko oblasti, kde se nacházejí obchody s oděvy a květinářství, které tyto reklamy zadávají, Nora okamžitě tyto reklamy uvidí.

1015 Pracovní skupina zřízená podle článku 29 (2009), *Stanovisko č. 5/2009 k internetovým sociálním sítím*, WP 163, 12. června 2009, s. 4.

1016 Rada Evropy, Výbor ministrů, Doporučení Výboru ministrů členským státům CM/Rec(2012)4 o ochraně lidských práv na sociálních sítích, 4. dubna 2012.

1017 Rada Evropy, Výbor ministrů, Důvodová zpráva, Doporučení Výboru ministrů členským státům Rec(2001)2 o Evropském kodexu policejní etiky, 7. března 2018.

Internet věcí

Internet věcí (IoT) představuje další krok ve vývoji internetu, éru webu 3.0. Internet věcí umožňuje, aby byly přístroje připojené a interagovaly s jinými přístroji přes internet. Díky tomu mohou být objekty a lidé vzájemně propojeni prostřednictvím komunikačních sítí, oznamovat svůj status a/nebo status okolního prostředí.[1018] Internet věcí a připojená zařízení jsou již skutečností a očekává se, že v příštích několika letech významně porostou s tím, jak budou vznikat a dále se rozvíjet chytrá zařízení, což povede ke vzniku chytrých měst, chytrých domácností a chytrých podniků.

Příklad: Internet věcí je zvlášť prospěšný v oblasti zdravotnictví. Podniky již vytvořily přístroje, senzory a aplikace, které umožňují sledování zdraví pacienta. Díky používání poplašného tlačítka nošeného na těle a jiných bezdrátových senzorů umístěných v domácnosti je možné sledovat každodenní činnosti seniorů, kteří žijí sami, a vyvolat poplach, pokud je zjištěno, že byl jejich denní program vážně narušen. Například starší lidé běžně používají senzory detekce pádu. Tyto senzory mohou s vysokou přesností zjistit pády a informovat o nich lékaře a/nebo rodinu dané osoby.

Příklad: Barcelona je jedním z nejznámějších příkladů chytrého města. Od roku 2012 zavedlo město používání inovativních technologií, které mají vytvořit inteligentní systém veřejné dopravy, nakládání s odpady, parkování a pouličního osvětlení. Například ke zlepšení nakládání s odpady používá město chytré odpadkové koše. Ty umožňují monitorovat objem odpadu s cílem optimalizovat trasy svozu. Když jsou tyto koše téměř plné, vyšlou signály prostřednictvím sítě mobilních komunikací, které jsou zaslány do softwarové aplikace používané společností zajišťující nakládání s odpady. Společnost tak může naplánovat nejlepší trasu pro svoz odpadu, stanovit priority a/nebo pouze zajistit svoz košů, které skutečně je třeba vyprázdnit.

10.2.2. Hledání rovnováhy mezi přínosy a riziky

Ohromné rozšíření a úspěch sociálních sítí v minulém desetiletí svědčí o tom, že přinášejí **významné výhody**. Například cílená reklama (jak je popsáno ve zvýrazněném příkladu) je mimořádně inovativní způsob, jak mohou podniky oslovit své

1018 Evropská komise, Pracovní dokument útvarů Komise, *Advancing the Internet of Things in Europe [Dosahování pokroku v oblasti internetu věcí v Evropě]*, SWD(2016) 110, 19. dubna 2016.

cílové skupiny, a nabízí jim konkrétnější trh. Může být i v zájmu spotřebitelů, aby jim prezentované reklamy byly relevantnější a zajímavější. Zejména však mohou mít sociální sítě a sociální média pozitivní dopad na společnost a na provádění změny. Zmocňují uživatele, aby komunikovali, interagovali, organizovali skupiny a akce na témata, která se jich dotýkají.

Obdobně se očekává, že internet věcí nabídne významné přínosy hospodářství, a je součástí strategie EU pro rozvoj jednotného digitálního trhu. Odhaduje se, že v rámci EU se v roce 2020 počet přístrojů připojených k internetu věcí zvýší na šest miliard. Tento nárůst konektivity podle očekávání zajistí významné hospodářské přínosy prostřednictvím vývoje inovativních služeb a aplikací, lepší zdravotní péče, lepšího porozumění potřebám spotřebitelů a větší účinnosti.

Současně vzhledem k obrovskému objemu osobních informací vytvořených uživateli sociálních médií a následně zpracovaných provozovateli služeb vyvolává rozšíření sociálních sítí **stále větší obavy** týkající se způsobů, jak je možné ochránit soukromí a osobní údaje. Sociální sítě mohou ohrožovat právo na soukromý život a právo na svobodu projevu. Mezi tyto hrozby může patřit: „nedostatek právních a procesních záruk týkajících se postupů, které mohou vést k vyloučení uživatelů; nedostatečná ochrana dětí a mladých lidí před škodlivým obsahem nebo chováním; nedodržování práv jiných osob; nedostatečné standardní nastavení vstřícné k ochraně soukromí; nedostatek transparentnosti, pokud jde o účely, za kterými jsou osobní údaje shromažďovány a zpracovávány.“[1019] Evropské právo v oblasti ochrany údajů se pokusilo reagovat na výzvy v oblasti ochrany soukromí/údajů, které přinesla sociální média. V souvislosti se sociálními médii a službami vytváření sítí jsou zvlášť důležité zásady, jako je souhlas, záměrná a standardní ochrana soukromí/údajů a práva jednotlivců.

V souvislosti s internetem věcí obrovský objem osobních údajů generovaných z různých propojených přístrojů také obnáší rizika pro ochranu soukromí a údajů. Ačkoliv transparentnost je důležitou zásadou evropského práva pro ochranu údajů, kvůli velkému počtu propojených přístrojů není vždy jasné, kdo může data shromážděná z přístrojů připojených k internetu věcí shromažďovat, přistupovat k nim a používat je.[1020] Podle práva EU a RE však zásada transparentnosti stanoví povinnost správců informovat subjekty údajů o tom, jak jsou jejich údaje používány, a to jasnými a srozumitelnými jazykovými prostředky. Dotčeným jednotlivcům musí být vyjasněna

1019 Rada Evropy, Doporučení členským státům Rec(2012)4 o ochraně lidských práv na sociálních sítích, 4. dubna 2012.

1020 Evropský inspektor ochrany údajů (2017), *Understanding the Internet of Things [Jak porozumět internetu věcí]*.

rizika, pravidla, záruky a práva, pokud jde o zpracování jejich osobních údajů. Přístroje připojené k internetu věcí a vícenásobné operace zpracování a dotčené údaje mohou také představovat výzvu pro požadavek na jasný a informovaný souhlas se zpracováním údajů – pokud je toto zpracování založeno na souhlasu. Jednotlivci často nerozumějí technickým aspektům fungování takovéhoto zpracování, a tedy ani důsledkům svého souhlasu.

Další významnou výzvou je zabezpečení, jelikož připojené přístroje jsou mimořádně zranitelné z hlediska bezpečnostních rizik. Míra zabezpečení se u jednotlivých připojených přístrojů liší. Jelikož se nejedná o standardní IT infrastrukturu, mohou postrádat dostatečnou výpočetní a úložnou kapacitu, a nemohou tedy mít bezpečnostní software nebo používat techniky, jako je šifrování, pseudonymizace nebo anonymizace, na ochranu osobních informací uživatelů.

Příklad: V Německu se regulátoři rozhodli zakázat hračku připojenou k internetu poté, co vyvolala silné obavy o dopadu hračky na dodržování práva na soukromý život dětí. Regulátoři měli za to, že panenka připojená k internetu s názvem Cayla fakticky představuje přístroj ke skrytému špehování. Panenka fungovala na principu zasílání otázek dítěte, které si s ní hraje, aplikaci na digitálním přístroji, který otázku přeložil do podoby textu a vyhledal odpověď na internetu. Aplikace následně zaslala odpověď panence, která ji přehrála dítěti. Pomocí této panenky bylo možné zaznamenávat a předávat aplikaci komunikaci dítěte, ale také komunikaci blízko se nacházejících dospělých. Pokud by výrobci panenky nepřijali dostatečná bezpečnostní opatření, mohla být panenka zneužita kýmkoliv k tomu, aby odposlouchával rozhovory.

10.2.3. Otázky související s ochranou údajů

Souhlas

Zpracování osobních údajů v Evropě je v souladu s právními předpisy pouze tehdy, pokud je umožněno evropským právem v oblasti ochrany údajů. V případě poskytovatelů sociálních sítí je zákonným základem pro zpracování údajů obvykle souhlas subjektů údajů. Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný (viz oddíl 4.1.1).[1021] „Svobodný“ v zásadě znamená, že subjekty údajů musí mít skutečnou a opravdovou volbu. Souhlas je „konkrétní“ a „informovaný“, pokud je

1021 Obecné nařízení o ochraně osobních údajů, článek 4 a 7; Modernizovaná úmluva č. 108, článek 5.

srozumitelný a jasně a přesně uvádí plný rozsah, účely a důsledky zpracování údajů. V souvislosti se sociálními médii je možné zpochybnit, zda je souhlas svobodný, konkrétní a informovaný u všech druhů zpracování, které provozovatel sociální sítě a třetí strany provádějí.

Příklad: Aby se jednotlivci mohli připojit na sociální síť nebo k ní získat přístup, musejí často souhlasit s různými druhy zpracování svých osobních údajů, často aniž by jim byly poskytnuty nezbytné upřesňující informace nebo alternativy. Příkladem může být povinnost souhlasit s příjmem behaviorálně cílené reklamy, aby se člověk mohl zaregistrovat na sociální síť. Jak konstatuje ve svém stanovisku k definici souhlasu pracovní skupina zřízená podle článku 29, „vzhledem k tomu, jakého významu některé sociální sítě nabyly, budou uživatelé určitých kategorií (například dospívající) s přijímáním behaviorálně cílené reklamy souhlasit, aby se vyhnuli riziku, že budou částečně vyloučeni ze sociálních interakcí. Uživateli by mělo být umožněno, aby udělil svobodný a výslovný souhlas s přijímáním behaviorálně cílené reklamy, nezávisle na jeho přístupu ke službě sociální sítě.“[1022]

Podle obecného nařízení o ochraně osobních údajů není v zásadě možné zpracovávat osobní údaje dětí mladších 16 let na základě jejich souhlasu.[1023] Pokud je souhlas pro zpracování nezbytný, musí jej udělit rodič nebo poručník dítěte. Děti vyžadují zvláštní ochranu kvůli tomu, že si mohou být méně vědomy rizik a důsledků spojených se zpracováním údajů. To je velmi důležité v souvislosti se sociálními médii, protože děti jsou zranitelnější vůči některým negativním účinkům, jež používání těchto médií může obnášet, jako je kyberšikana, kybernetické pronásledování nebo krádež identity.

Bezpečnost a soukromí / záměrná a standardní ochrana údajů

Zpracování osobních údajů nevyhnutelně obnáší bezpečnostní rizika vzhledem k neustálé možnosti porušení zabezpečení, které povede k nezáměrnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění zpracovávaných osobních údajů. Podle evropského práva v oblasti ochrany údajů jsou správci a zpracovatelé povinni zavést vhodná technická a organizační

1022 Pracovní skupina zřízená podle článku 29 (2011), *Stanovisko č. 15/2011 k definici souhlasu*, WP 187, 13. července 2011, s. 18.

1023 Viz obecné nařízení o ochraně osobních údajů, článek 8. Členské státy EU mohou právním předpisem stanovit nižší věk, ne však nižší než 13 let.

opatření s cílem zabránit neoprávněnému zásahu do operací zpracování údajů. Tuto povinnost musí plnit také poskytovatelé sociálních sítí spadající do oblasti působnosti evropských pravidel v oblasti ochrany údajů.

Zásady záměrné a standardní ochrany soukromí/údajů vyžadují, aby správci zajišťovali zabezpečení již v návrhu svých produktů a aby automaticky uplatňovali vhodné nastavení v oblasti soukromí a ochrany údajů. To znamená, že pokud se určitá osoba rozhodne připojit se k sociální síti, nemusí poskytovatel služby automaticky zpřístupnit veškeré informace o novém uživateli služby všem svým uživatelům. V okamžiku, kdy se daná osoba připojí ke službě, by standardní nastavení ochrany soukromí a údajů mělo být takové, aby byly informace k dispozici pouze vybraným kontaktům dané osoby. Rozšíření přístupu k těmto informacím na lidi, kteří nejsou uvedeni na tomto seznamu, by mělo být možné až poté, co uživatel manuálně změní standardní nastavení ochrany soukromí a údajů. To může mít rovněž dopad v případech, kdy dojde k porušení zabezpečení, a to navzdory zavedeným bezpečnostním opatřením. V takovýchto případech musí poskytovatelé služby informovat dotčené uživatele, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody subjektů údajů.[1024]

Záměrná a standardní ochrana osobních údajů jsou zvlášť důležité v souvislosti se sociálními sítěmi, jelikož vedle rizika neoprávněného přístupu, které je obsaženo ve většině druhů zpracování, představuje další bezpečnostní rizika sdílení osobních údajů na sociálních médiích. K tomu často dochází proto, že jednotlivci neporozumí tomu, *kdo* může mít k jejich informacím přístup a jak je tito lidé mohou používat. S tím, jak se používání sociálních médií rozšířilo, se zvýšil i počet incidentů a obětí krádeže identity.

Příklad: Krádež identity je jev, kdy osoba získá informace, údaje nebo dokumenty patřící jiné osobě (oběti) a pak tyto informace použije k tomu, aby se za oběť vydávala za účelem získání výrobků nebo služeb jménem oběti. Vezměme si například Paula, který má účet na webové stránce sociálních médií. Paul je učitel a aktivní člen své komunity, je velmi společenský a nemá zvláštní obavy ohledně nastavení ochrany soukromí a údajů na svém účtu sociálních médií. Má velký adresář kontaktů, někdy včetně lidí, které nemusí nevyhnutelně znát osobně. Protože pracuje ve velké škole a je poměrně populární trenér školního fotbalového mužstva, myslí si, že tito lidé jsou

1024 Tamtéž, článek 34.

nejspíše rodiče nebo přátelé školy. Na jeho účtu sociálních médií jsou zobrazeny Paulova e-mailová adresa a narozeniny. Kromě toho Paul pravidelně zveřejňuje fotografie svého psa Tobyho spolu s komentářem jako „Já a Toby při ranním běhu". Paul si neuvědomil, že jednou z nejoblíbenějších bezpečnostních otázek na ochranu jeho e-mailu nebo účtu na mobilním telefonu je „jak se jmenuje vaše domácí zvíře". S pomocí informací dostupných na Paulově profilu na sociálních médiích Nick dokázal snadno neoprávněně proniknout k Paulovým účtům.

Práva jednotlivců

Poskytovatelé sociálních sítí musí dodržovat práva jednotlivců (viz oddíl 6.1), včetně práva být informován o účelu zpracování a o tom, jak mohou být osobní údaje použity pro účely přímého marketingu. Jednotlivcům musí být rovněž přiznáno právo na přístup k osobním údajům, které vytvořili na platformě sociální sítě, a právo požádat o jejich výmaz. I v případě, že osoby souhlasily se zpracováním osobních údajů a informací nahraných na internet, měly by mít možnost požádat o to, aby „byly zapomenuty", pokud již nechtějí využívat služby dané sociální sítě. Právo na přenositelnost údajů dále umožňuje uživatelům získat kopii osobních údajů, které poskytli poskytovateli sociálních sítí, ve strukturovaném, běžně používaném a strojově čitelném formátu, a předat tyto údaje od jednoho poskytovatele sociálních sítí jinému.[1025]

Správci

Složitou otázkou, která často vyvstává v souvislosti se sociálními médii, je, kdo je správce, tedy: kdo je osoba, která má povinnost a odpovědnost za soulad s pravidly ochrany údajů. Podle evropského práva v oblasti ochrany údajů se za správce považují poskytovatelé sociálních sítí. To jasně vyplývá z široké definice pojmu „správce" a ze skutečnosti, že tito poskytovatelé služeb určují účel a prostředky zpracování osobních údajů sdílených jednotlivci. Podle práva EU jsou správci, pokud nabízejí služby subjektům údajů v EU, povinni jednat v souladu s ustanoveními obecného nařízení o ochraně osobních údajů, a to i když nejsou usazeni v EU.

Je však možné považovat za správce také uživatele sociálních sítí? Pokud uživatelé zpracovávají osobní údaje „v rámci činnosti čistě osobní povahy nebo činnosti

1025 Obecné nařízení o ochraně osobních údajů, článek 21.

prováděné výhradně v domácnosti“, pravidla ochrany údajů se nepoužijí. Toto ustanovení se v evropském právu v oblasti ochrany údajů označuje jako „výjimka pro domácnosti“. Avšak v některých případech se na uživatele sociální sítě nemusí výjimka pro domácnosti vztahovat.

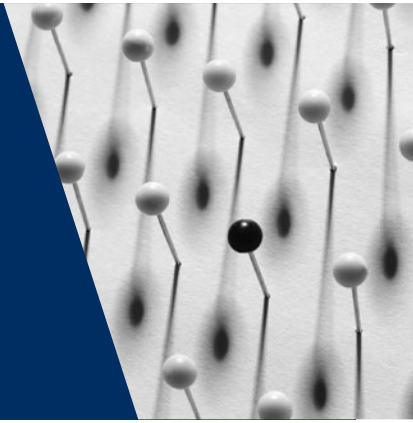
Uživatelé dobrovolně sdílejí své osobní informace on-line. Avšak informace sdílené on-line často obsahují osobní informace o jiných jednotlivcích.

Příklad: Paul má účet na velmi oblíbené platformě sociální sítě. Snaží se stát hercem a používá svůj účet ke zveřejňování fotografií, videí a příspěvků, v nichž vysvětluje své nadšení pro umění. Pro jeho budoucnost je popularita velmi důležitá; musí se tedy rozhodnout, zda by měl být jeho profil dostupný nejen úzkému okruhu jeho kontaktů, ale všem uživatelům internetu, ať už jsou členy sítě, nebo ne. Může Paul zveřejnit fotografie a videa zachycující jeho a jeho přítelkyni Sarah bez jejího souhlasu? Sarah, učitelka na základní škole, se snaží svůj soukromý život chránit před svým zaměstnavatelem, žáky a jejich rodiči. Představme si situaci, kdy Sarah, která nepoužívá sociální sítě, zjistí od jejich společného kamaráda Nicka, že fotografie, na které je zachycena na večírku s Paulem, byla zveřejněna on-line. V takovém případě zpracování údajů ze strany Paula nespadá podle práva EU mezi činnosti, na které se vztahuje „výjimka pro domácnosti“.

Je však důležité, aby si uživatelé byli vědomi a měli na paměti, že nahrávání informací o jiných jednotlivcích bez jejich souhlasu může představovat porušení práv těchto jednotlivců na ochranu soukromí a údajů. I v případě, že se na danou situaci bude vztahovat „výjimka pro domácnosti“ – například pokud má uživatel profil, který byl zveřejněn seznamu kontaktů, které sám zvolil –, přesto může nést odpovědnost za zveřejnění osobních informací o jiných osobách. Ačkoliv pravidla ochrany údajů by se v případě použití výjimky pro domácnosti nepoužila, může vyvstat odpovědnost na základě uplatnění jiných vnitrostátních předpisů, jako je pomluva nebo porušení práva na ochranu osobnosti. V neposlední řadě jsou chráněni výjimkou pro domácnosti pouze uživatelé sociálních sítí: správci a zpracovatelé, kteří poskytují prostředky pro toto soukromé zpracování, spadají do působnosti práva EU na ochranu údajů.[1026]

1026 Tamtéž, 18. bod odůvodnění.

Po reformě směrnice o soukromí a elektronických komunikacích by se pravidla pro ochranu údajů a soukromí a bezpečnostní pravidla, která se vztahují na poskytovatele telekomunikačních služeb podle současného právního rámce, vztahovala rovněž na komunikaci mezi stroji a služby elektronických komunikacích, včetně například služeb „over the top".



Další literatura

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*, Vídeň, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance" [Čtyři základní práva: hledání rovnováhy], *International Data Privacy Law*, roč. 6, č. 3, s. 195–209.

EDRi, *An introduction to data protection* [Úvod do ochrany údajů], Brusel.

Frowein, J. a Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

González Fuster, G. a Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right" [Základní právo na ochranu údajů v Evropské unii: hledání neprozkoumaného práva], *International Review of Law, Computers and Technology*, roč. 26, č. 1, s. 73–82.

Grabenwarter, C. a Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Mnichov, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. a Nouwt, S. (eds.) (2009), *Reinventing Data Protection* [Změna koncepce ochrany údajů], Springer.

Harris, D., O'Boyle, M., Warbrick, C. a Bates, E. (2009), *Law of the European Convention on Human Rights* [Právo podle Evropské úmluvy o lidských právech], Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU* [Evropská unie jako strážkyně ochrany soukromí na internetu – příběh článku 16 SFEU], Springer.

Hustinx, P. (2016), „EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation" [Právo EU v oblasti ochrany údajů: přezkum směrnice 95/46/ES a navrhovaného obecného nařízení o ochraně osobních údajů].

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Mnichov, C. H. Beck.

Kokott, J. a Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR" [Rozlišování mezi ochranou soukromí a ochranou údajů v judikatuře SDEU a ESLP], *International Data Privacy Law*, roč. 3, č. 4, s. 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten" [Google a právo být zapomenut], *European Data Protection Law Review*, roč. 1, č. 1, s. 70–79.

Lynskey, O. (2014), „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order" [Dekonstrukce ochrany údajů: „přidaná hodnota" práva na ochranu údajů v právním řádu EU], *International and Comparative Law Quarterly*, roč. 63, č. 3, s. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law* [Základy práva EU v oblasti ochrany údajů], Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights* [Věci, materiály a komentář týkající se Evropské úmluvy o lidských právech], Oxford, Oxford University Press.

Nowak, M., Januszewski, K. a Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights* [Všechna lidská práva pro všechny – Vídeňská příručka k lidským právům], Antverpy, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. a Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brusel, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, č. 5, s. 281–288.

Warren, S. a Brandeis, L. (1890), „The right to privacy" [Právo na soukromí], *Harvard Law Review,* roč. 4, č. 5, s. 193–220.

White, R. a Ovey, C. (2010), *The European Convention on Human Rights* [Evropská úmluva o lidských právech], Oxford, Oxford University Press.

Kapitola 2

Acquisty, A., a Gross R. (2009), „Predicting Social Security numbers from public data" [Predikce čísel sociálního zabezpečení na základě veřejných údajů], *Proceedings of the National Academy of Science*, 7. července 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law* [Ochrana údajů: Praktická příručka pro právo Spojeného království a EU], Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. a Blondel V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility" [Jedinečný v davu: Hranice lidské mobility z hlediska soukromí], *Nature Scientific Reports*, roč. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paříž, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU* [Formování ochrany osobních údajů jako základního práva v EU], Springer.

Morgan, R. a Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance* [Strategie ochrany údajů: Zavádění dodržování ochrany údajů], Londýn, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“ [Porušené sliby soukromí: Reakce na překvapivé selhání anonymizace], *UCLA Law Review*, roč. 57, č. 6, s. 1701–1777.

Samarati, P. a Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression“ [Ochrana soukromí při zpřístupňování informací: k-anonymita a její vynucování zobecňováním a potlačováním], technická zpráva SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy“ [K-anonymita: model na ochranu soukromí] *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, roč. 10, č. 5, s. 557–570.

Tinnefeld, M., Buchner, B. a Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Mnichov, Oldenbourg Wissenschaftsverlag.

Úřad komisaře pro informace Spojeného království (2012), Anonymisation: managing data protection risk. *Code of practice [Anonymizace: řízení rizik spojených s ochranou údajů. Kodex správné praxe]*.

Kapitoly 3 až 6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ in: Grabitz, E., Hilf, M. a Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Mnichov, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. a Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?“ [Odvolání souhlasu: „mrtvý bod“ v právu v oblasti ochrany údajů], *Computer Law & Security Review*, roč. 26, č. 3, s. 273–283.

Dammann, U. a Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. a Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis" [Směrnice o ochraně údajů policií a trestním soudnictvím: komentář a analýza], *Computers & Law Magazine of SCL*, roč. 22, č. 6, s. 1–5.

De Hert, P. a Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals" [Navrhované nařízení o ochraně údajů nahrazující směrnici 95/46/ES: solidní systém pro ochranu jednotlivců], *Computer Law & Security Review*, roč. 28, č. 2, s. 130–142.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously" [Evropský pohled na souhlas se zpracováním údajů prostřednictvím rekonceptualizace evropského náhledu na ochranu údajů po Lisabonské smlouvě: bereme práva vážně], *European Review of Private Law*, roč. 20, č. 2, s. 473–506.

FRA (Agentura Evropské unie pro základní práva) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)* [Ochrana údajů v Evropské unii: Úloha vnitrostátních orgánů pro ochranu údajů (Posilování architektury základních práv v EU II)], Lucemburk, Úřad pro publikace Evropské unie (Úřad pro publikace).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* [Vývoj ukazatelů ochrany, respektování a podporování práv dítěte v Evropské unii] (vydání určené pro konferenci), Vídeň, FRA.

FRA (2011), Access to justice in Europe: an overview of challenges and opportunities [Přístup ke spravedlnosti v Evropě: Přehled problémů a příležitostí], Lucemburk, Úřad pro publikace.

Irský orgán pro informace o zdraví a kvalitu zdraví (2010), Guidance on Privacy Impact Assessment in Health and Social Care [Pokyny týkající se posouzení vlivu na soukromí v odvětví zdravotní a sociální péče].

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. a Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108" [O 30 let později – přezkum Úmluvy Rady Evropy o ochraně údajů], *Computer Law & Security Review*, roč. 27, č. 3, s. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

Úřad komisaře pro informace Spojeného království, Privacy Impact Assessment [Posouzení vlivu na soukromí].

Kapitola 7

Pracovní skupina zřízená podle článku 29 (2005), *Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995*.

Evropský inspektor ochrany údajů (2014), The transfer of personal data to third countries and international organisations by EU institutions and bodies [Stanovisko k předávání osobních údajů ze strany orgánů a institucí EU třetím zemím a mezinárodním organizacím].

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. a Nouwt, S. (2009), *Reinventing data protection?* [Hledání nové koncepce ochrany údajů?], Berlín, Springer.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law* [Regulace předávání údajů do zahraničí a právo v oblasti ochrany údajů], Oxford, Oxford University Press

Kuner, C. (2007), *European data protection law* [Evropské právo v oblasti ochrany údajů], Oxford, Oxford University Press.

Kapitola 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective* [Celosvětová ochrana údajů v oblasti prosazování práva, pohled EU], Londýn, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level* [Sdílení informací a ochrana údajů v prostoru svobody, bezpečnosti a práva. Na cestě k harmonizovaným zásadám ochrany údajů pro výměnu informací na úrovni EU], Berlín, Springer.

De Hert, P. a Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis“ [Směrnice o ochraně údajů policií a trestním soudnictvím: komentář a analýza], *Computers & Law Magazine of SCL*, roč. 22, č. 6, s. 1–5.

Drewer, D. a Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime“ [Rámec Europolu pro ochranu údajů jako přínos v boji proti kyberkriminalitě], *ERA Forum*, roč. 13, č. 3, s. 381–395.

Eurojust (2014), *Data protection at Eurojust: A robust, effective and tailor-made regime* [Ochrana údajů v Eurojustu: Spolehlivý, účinný a na míru vytvořený režim], Haag, Eurojust.

Europol (2012), *Data Protection at Europol* [Ochrana údajů v Europolu], Lucemburk, Úřad pro publikace.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe* [Výměna informací a ochrana údajů v přeshraničních trestních řízeních v Evropě], Berlín, Springer.

Gutwirth, S., Poullet, Y. a De Hert, P. (2010), *Data protection in a profiled world* [Ochrana údajů v profilovaném světě], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. a Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* [Počítače, soukromí a ochrana údajů: Prvek volby], Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem“ [Ničíme demokracii z důvodu její ochrany? Směrnice o uchovávání údajů, stát sledující obyvatele a náš ústavní ekosystém], *European Law Review*, roč. 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* [Úloha Evropského parlamentu při uzavírání transatlantických dohod o předávání osobních údajů po Lisabonu], Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Kapitola 9

Büllesbach, A., Gijrath, S., Poullet, Y. a Hacon, R. (2010), *Concise European IT law* [Přehled evropského práva v oblasti informačních technologií], Amsterdam, Kluwer Law International.

Gutwirth, S., Poullet, Y. a De Hert, P. (2010), *Data protection in a profiled world* [Ochrana údajů v profilovaném světě], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. a Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* [Počítače, soukromí a ochrana údajů: Prvek volby], Dordrecht, Springer.

Gutwirth, S., Leenes, R., De Hert, P. a Poullet, Y. (2012), *European data protection: In good health?* [Ochrana údajů v Evropě: Je v dobrém stavu?], Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem" [Ničíme demokracii z důvodu její ochrany? Směrnice o uchovávání údajů, stát sledující obyvatele a náš ústavní ekosystém], *European Law Review*, roč. 36, č. 5, s. 722–776.

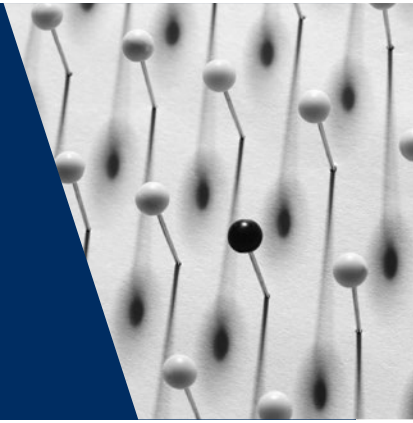
Rosemary, J. a Hamilton, A. (2012), *Data protection law and practice* [Právo a praxe v oblasti ochrany údajů], Londýn, Sweet & Maxwell.

Kapitola 10

El Emam, K. a Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques" [Kritické hodnocení stanoviska č. 5/2014 k technikám anonymizace pracovní skupiny zřízené podle článku 29], *International Data Privacy Law*, roč. 5, č. 1, s. 73–87.

Mayer-Schönberger, V. a Cate, F. (2013), „Notice and consent in a world of Big Data" [Oznamování a souhlas ve světě dat velkého objemu], *International Data Privacy Law*, roč. 3, č. 2, s. 67–73.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?" [Data velkého objemu: Konec soukromí nebo nový začátek], *International Data Privacy Law*, roč. 3, č. 2, s. 74–87.



Judikatura

Vybraná judikatura Evropského soudu pro lidská práva

Přístup k osobním údajům
Gaskin v. Spojené království, č. 10454/83, 7. července 1989
Godelli v. Itálie, č. 33783/09, 25. září 2012
K.H. a další v. Slovensko, č. 32881/04, 28. dubna 2009
Leander v. Švédsko, č. 9248/81, 26. března 1987
M.K. v. Francie, č. 19522/09, 18. dubna 2013
Odièvre v. Francie, velký senát, č. 42326/98, 13. února 2003

Hledání rovnováhy mezi ochranou údajů a svobodou projevu a právem na informace
Axel Springer AG v. Německo, velký senát, č. 39954/08, 7. února 2012
Bohlen v. Německo, č. 53495/09, 19. února 2015
Coudec a Hachette Filipacchi Associés v. Francie, velký senát, č. 40454/07, 10. listopadu 2015
Magyar Helsinki Bizottság v. Maďarsko, velký senát, č. 18030/11, 8. listopadu 2016
Müller a další v. Švýcarsko, č. 10737/84, 24. května 1988
Satakunnan Markkinapörssi Oy a Satamedia Oy v. Finsko, velký senát, č. 931/13, 27. června 2017
Vereinigung bildender Künstler v. Rakousko, č. 68345/01, 25. ledna 2007
Von Hannover v. Německo (č. 2), velký senát, č. 40660/08 a 60641/08, 7. února 2012

Hledání rovnováhy mezi ochranou údajů a svobodou náboženství
Sinan Işık v. Turecko, č. 21924/05, 2. února 2010

Výzvy v oblasti on-line ochrany údajů
K.U. v. Finsko, č. 2872/02, 2. prosince 2008

Souhlas subjektu údajů
Elberte v. Lotyšsko, č. 61243/08, 13. ledna 2015
Sinan Işık v. Turecko, č. 21924/05, 2. února 2010
Y. v. Turecko, č. 648/10, 17. února 2015

Korespondence
Amann v. Švýcarsko, velký senát, č. 27798/95, 16. února 2000
Association for European Integration and Human Rights a Ekimdzhiev v. Bulharsko, č. 62540/00, 28. června 2007
Bernh Larsen Holding AS a další v. Norsko, č. 24117/08, 14. března 2013
Cemalettin Canli v. Turecko, č. 22427/04, 18. listopadu 2008
D.L. v. Bulharsko, č. 7472/14, 19. května 2016
Dalea v. Francie, č. 964/07, 2. února 2010
Gaskin v. Spojené království, č. 10454/83, 7. července 1989
Haralambie v. Rumunsko, č. 21737/03, 27. října 2009
Khelili v. Švýcarsko, č. 16188/07, 18. října 2011
Leander v. Švédsko, č. 9248/81, 26. března 1987
Malone v. Spojené království, č. 8691/79, 2. srpna 1984
Rotaru v. Rumunsko, velký senát, č. 28341/95, 4. května 2000
S. a Marper v. Spojené království, velký senát, č. 30562/04 a 30566/04, 4. prosince 2008
Shimovolos v. Rusko, č. 30194/09, 21. června 2011
Silver a další v. Spojené království, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25. března 1983
The Sunday Times v. Spojené království, č. 6538/74, 26. dubna 1979

Databáze rejstříků trestů
Aycaguer v. Francie, č. 8806/12, 22. června 2017
B.B. v. Francie, č. 5335/06, 17. prosince 2009
Brunet v. Francie, č. 21010/10, 18. září 2014
M.K. v. Francie, č. 19522/09, 18. dubna 2013
M.M. v. Spojené království, č. 24029/07, 13. listopadu 2012

Bezpečnost údajů
Haralambie v. Rumunsko, č. 21737/03, 27. října 2009
K.H. a další v. Slovensko, č. 32881/04, 28. dubna 2009

Databáze DNA
S. a Marper v. Spojené království, velký senát, č. 30562/04 a 30566/04, 4. prosince 2008

Údaje z GPS
Uzun v. Německo, č. 35623/05, 2. září 2010

Zdravotní údaje
Avilkina a další v. Rusko, č. 1585/09, 6. června 2013
Biriuk v. Litva, č. 23373/03, 25. listopadu 2008
I. v. Finsko, č. 20511/03, 17. července 2008
L.H. v. Lotyšsko, č. 52019/07, 29. dubna 2014
L.L. v. Francie, č. 7508/02, 10. října 2006
M.S. v. Švédsko, č. 20837/92, 27. srpna 1997
Szuluk v. Spojené království, č. 36936/05, 2. června 2009
Y. v. Turecko, č. 648/10, 17. února 2015
Z. v. Finsko, č. 22009/93, 25. února 1997

Totožnost
Ciubotaru v. Moldavsko, č. 27138/04, 27. dubna 2010
Godelli v. Itálie, č. 33783/09, 25. září 2012
Odièvre v. Francie, velký senát, č. 42326/98, 13. února 2003

Informace týkající se profesionální činnosti
G.S.B. v. Švýcarsko, č. 28601/11, 22. prosince 2015
M.N. a další v. San Marino, č. 28005/12, 7. července 2015
Michaud v. Francie, č. 12323/11, 6. prosince 2012
Niemietz v. Německo, č. 13710/88, 16. prosince 1992

Odposlouchávání komunikace
Amann v. Švýcarsko, velký senát, č. 27798/95, 16. února 2000
Brito Ferrinho Bexiga Villa-Nova v. Portugalsko, č. 69436/10, 1. prosince 2015
Copland v. Spojené království, č. 62617/00, 3. dubna 2007
Halford v. Spojené království, č. 20605/92, 25. června 1997
Iordachi a další v. Moldavsko, č. 25198/02, 10. února 2009

Kopp v. Švýcarsko, č. 23224/94, 25. března 1998
Liberty a další v. Spojené království, č. 58243/00, 1. července 2008
Malone v. Spojené království, č. 8691/79, 2. srpna 1984
Mustafa Sezgin Tanrıkulu v. Turecko, č. 27473/06, 18. července 2017
Pruteanu v. Rumunsko, č. 30181/05, 3. února 2015
Szuluk v. Spojené království, č. 36936/05, 2. června 2009

Povinnosti povinných subjektů
B.B. v. Francie, č. 5335/06, 17. prosince 2009
I. v. Finsko, č. 20511/03, 17. července 2008
Mosley v. Spojené království, č. 48009/08, 10. května 2011

Osobní údaje
Amann v. Švýcarsko, velký senát, č. 27798/95, 16. února 2000
Bernh Larsen Holding AS a další v. Norsko, č. 24117/08, 14. března 2013
Uzun v. Německo, č. 35623/05, 2010

Fotografie
Sciacca v. Itálie, č. 50774/99, 11. ledna 2005
Von Hannover v. Německo, č. 59320/00, 24. června 2004

Právo být zapomenut
Satakunnan Markkinapörssi Oy a Satamedia Oy v. Finsko, velký senát, č. 931/13, 27. června 2017
Segerstedt-Wiberg a další v. Švédsko, č. 62332/00, 6. června 2006

Právo vznést námitku
Leander v. Švédsko, č. 9248/81, 26. března 1987
M.S. v. Švédsko, č. 20837/92, 27. srpna 1997
Mosley v. Spojené království, č. 48009/08, 10. května 2011
Rotaru v. Rumunsko, velký senát, č. 28341/95, 4. května 2000
Sinan Işık v. Turecko, č. 21924/05, 2. února 2010

Citlivé kategorie údajů
Brunet v. Francie, č. 21010/10, 18. září 2014
I. v. Finsko, č. 20511/03, 17. července 2008
Michaud v. Francie, č. 12323/11, 6. prosince 2012
S. a Marper v. Spojené království, velký senát, č. 30562/04 a 30566/04, 4. prosince 2008

Dohled a vynucování (úloha jednotlivých subjektů, včetně dozorových úřadů)
I. v. Finsko, č. 20511/03, 17. července 2008
K.U. v. Finsko, č. 2872/02, 2. prosince 2008
Von Hannover v. Německo, č. 59320/00, 24. června 2004
Von Hannover v. Německo (č. 2), velký senát, č. 40660/08 a 60641/08, 7. února 2012

Metody sledování
Allan v. Spojené království, č. 48539/99, 5. listopadu 2002
Association for European Integration and Human Rights a Ekimdzhiev v. Bulharsko, č. 62540/00, 28. června 2007
Bărbulescu v. Rumunsko, velký senát, č. 61496/08, 5. září 2017
D.L. v. Bulharsko, č. 7472/14, 19. května 2016
Dragojević v. Chorvatsko, č. 68955/11, 15. ledna 2015
Karabeyoğlu v. Turecko, č. 30083/10, 7. června 2016
Klass a další v. Německo, č. 5029/71, 6. září 1978
Roman Zakharov v. Rusko, velký senát, č. 47143/06, 4. prosince 2015
Rotaru v. Rumunsko, velký senát, č. 28341/95, 4. května 2000
Szabó a Vissy v. Maďarsko, č. 37138/14, 12. ledna 2016
Taylor-Sabori v. Spojené království, č. 47114/99, 22. října 2002
Uzun v. Německo, č. 35623/05, 2. září 2010
Versini-Campinchi a Crasnianski v. Francie, č. 49176/11, 16. června 2016
Vetter v. Francie, č. 59842/00, 31. května 2005
Vukota-Bojić v. Švýcarsko, č. 61838/10, 18. října 2016

Sledování videokamerou
Köpke v. Německo (dec.), č. 420/07, 5. října 2010
Peck v. Spojené království, č. 44647/98, 28. ledna 2003

Vzorky hlasů
P.G. a J.H. v. Spojené království, č. 44787/98, 25. září 2001
Wisse v. Francie, č. 71611/01, 20. prosince 2005

Vybraná judikatura Soudního dvora Evropské unie

Judikatura týkající se směrnice o ochraně údajů

Spojené věci C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24. listopadu 2011
[Správné provádění čl. 7 písm. f) směrnice o ochraně údajů – „oprávněné zájmy jiných osob" – ve vnitrostátním právu]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, 16. února 2012
[Povinnost poskytovatelů sociálních sítí zabránit protiprávnímu používání hudebních a audiovizuálních děl ze strany uživatelů sítě]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9. března 2017
[Právo na výmaz osobních údajů; právo vznést námitku proti zpracování]

C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*, 7. května 2009
[Právo subjektu údajů na přístup]

C-101/01, *Trestní řízení proti Bodil Lindqvist*, 6. listopadu 2003
[Zvláštní kategorie osobních údajů]

C-543/09, *Deutsche Telekom AG v. Bundesrepublik Deutschland*, 5. května 2011
[Nutnost obnovení souhlasu]

Spojené věci C-293/12 a C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, velký senát, 8. dubna 2014
[Porušení primárního práva EU ze strany směrnice o uchovávání údajů; zákonné zpracování; účelové omezení a omezení uložení]

C-518/07, *Evropská komise v. Spolková republika Německo*, velký senát, 9. března 2010
[Nezávislost vnitrostátního dozorového úřadu]

C-288/12, *Evropská komise v. Maďarsko*, velký senát, 8. dubna 2014
[Legitimnost odvolání z funkce vnitrostátního inspektora ochrany údajů]

C-614/10, *Evropská komise v. Rakouská republika*, velký senát, 16. října 2012
[Nezávislost vnitrostátního dozorového úřadu]

C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11. prosince 2014
[Pojmy „zpracování údajů" a „správce"]

C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, velký senát, 13. května 2014
[Povinnost poskytovatelů vyhledávačů zamezit na žádost subjektu údajů zobrazování osobních údajů ve výsledcích vyhledávání; použitelnost směrnice o ochraně údajů; pojem „zpracování údajů"; význam pojmu „správci"; vyvážení ochrany údajů a svobody projevu; právo být zapomenut]

C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, velký senát, 16. prosince 2008
[Oprávněné držení údajů o cizincích v registru pro statistické účely]

C-473/12, *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert a další*, 7. listopadu 2013
[Právo být informován o zpracování osobních údajů]

C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, velký senát, 6. října 2015
[Zásada zákonného zpracování; základní práva; neplatnost rozhodnutí o „bezpečném přístavu"; pravomoci nezávislých dozorových úřadů]

C-291/12, *Michael Schwarz v. Stadt Bochum*, 17. října 2013
[Řízení o předběžné otázce; oblast svobody, bezpečnosti a práva; biometrický cestovní pas, otisky prstů; právní základ; proporcionalita]

C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19. října 2016
[Definice „osobních údajů"; adresy internetového protokolu; ukládání dat poskytovatelem on-line mediálních služeb; vnitrostátní právní předpisy, které neumožňují zohlednění legitimního zájmu, který sleduje správce]

C-434/16, *Peter Nowak v. Data Protection Commissioner*, Stanovisko generální advokátky Kokottové, 20. července 2017
[Pojem osobních údajů; přístup k vlastním odpovědím na zkušební otázky; korekturní poznámky zkoušejícího]

T-462/12 R, *Pilkington Group Ltd v. Evropská komise*, usnesení předsedy Tribunálu, 11. března 2013

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, velký senát, 29. ledna 2008
[Pojem „osobní údaje"; povinnost poskytovatelů přístupu k internetu zpřístupnit totožnost uživatelů programů na výměnu souboru KaZaA sdružení zabývajícímu se ochranou duševního vlastnictví]

Spojené věci C-465/00, C-138/01 a C-139/01, *Rechnungshof v. Österreichischer Rundfunk a další a Christa Neukomm a Jospeh Lauermann v. Österreichischer Rundfunk*, 20. května 2003
[Přiměřenost právní povinnosti zveřejnit osobní údaje o platech zaměstnanců určitých kategorií institucí veřejného sektoru]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. listopadu 2011
[Informační společnost; autorské právo; internet; software „peer-to-peer"; poskytovatelé internetových služeb; instalace systému pro filtrování elektronických komunikací s cílem zabránit sdílení souborů, které porušují autorské právo; neexistence obecné povinnosti dohledu nad přenášenými informacemi]

C-201/14, *Smaranda Bara a další v. Casa Națională de Asigurări de Sănătate a další*, 1. října 2015
[Právo být informován o zpracování osobních údajů]

Spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Tom Watson a další*, velký senát, 21. prosince 2016
[Důvěrnost elektronických komunikací; poskytovatelé služeb elektronických komunikací; povinnost plošného a nediferencovaného uchovávání provozních a lokačních údajů; neexistence předchozího přezkumu ze strany soudu nebo nezávislého správního orgánu; Listina základních práv Evropské unie; slučitelnost s právem EU]

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy a Satamedia Oy*, velký senát, 16. prosince 2008
[Pojem „žurnalistické činnosti" ve smyslu článku 9 směrnice o ochraně údajů]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme"*, 4. května 2017
[Zásada zákonného zpracování: legitimní zájem sledovaný třetí stranou]

Spojené věci C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert v. Land Hessen*, velký senát, 9. listopadu 2010
[Pojem „osobní údaje"; přiměřenost právní povinnosti zveřejnit osobní údaje o příjemcích v rámci některých zemědělských fondů EU]

C-230/14, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1. října 2015
[Pravomoci vnitrostátních dozorových úřadů]

C-342/12, *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30. května 2013
[Pojem „osobní údaje"; evidence pracovní doby; zásady pro kvalitu údajů a kritéria oprávněnosti zpracování údajů; přístup vnitrostátního orgánu příslušného pro dohled nad pracovními podmínkami; povinnost zaměstnavatele zpřístupnit evidenci pracovní doby tak, aby bylo možné do ní bezprostředně nahlédnout]

Spojené věci C-141/12 a C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel a Minister voor Immigratie, Integratie en Asiel v. M a S*, 17. července 2014
[Oblast působnosti práva na přístup subjektu údajů; ochrana jednotlivců s ohledem na zpracování osobních údajů; pojem „osobní údaje"; údaje týkající se žadatele o povolení k pobytu a právní analýza obsažená ve správním dokumentu, který je přípravou pro rozhodnutí; Listina základních práv Evropské unie]

Judikatura týkající se směrnice (EU) 2016/681

Posudek 1/15 Soudního dvora (velkého senátu), 26. července 2017
[Právní základ; návrh dohody mezi Kanadou a Evropskou unií o předávání a zpracovávání údajů jmenné evidence cestujících; slučitelnost návrhu dohody s článkem 16 SFEU a články 7 a 8 a čl. 52 odst. 1 Listiny základních práv Evropské unie]

Judikatura týkající se nařízení o ochraně údajů orgány EU

C-615/13 P, ClientEarth, Pesticide Action Network Europe (PAN Europe) v. Evropský úřad pro bezpečnost potravin (EFSA), Evropská komise, 16. července 2015
[Přístup k dokumentům]

C-28/08 P, *Evropská komise v. The Bavarian Lager Co. Ltd.*, velký senát, 29. června 2010
[Přístup k dokumentům]

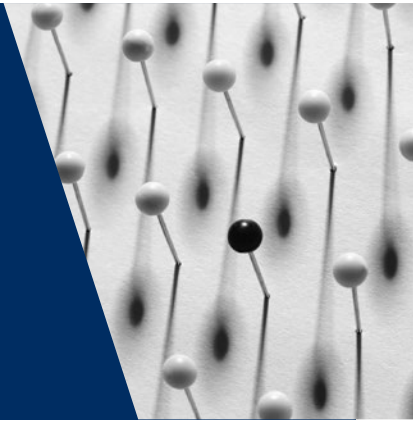
Judikatura týkající se směrnice 2002/58/ES

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*, 19. dubna 2012
[Autorské právo a práva s ním související; zpracování údajů prostřednictvím internetu; zásah do výlučného práva; audioknihy zpřístupněné na internetu prostřednictvím serveru FTP z IP adresy poskytnuté poskytovatelem internetového připojení; soudní příkaz určený poskytovateli internetového připojení sdělit jméno a adresu uživatele IP adresy]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24. listopadu 2011
[Informační společnost; autorské právo; internet; software „peer-to-peer"; poskytovatelé internetových služeb; instalace systému pro filtrování elektronických komunikací s cílem zabránit sdílení souborů, které porušují autorské právo; neexistence obecné povinnosti dohledu nad přenášenými informacemi]

C-536/15, *Tele2 (Netherlands) BV a další v. Autoriteit Consument en Markt (AMC)*, 15. března 2017
[Zásada zákazu diskriminace; předání osobních údajů účastníků pro účely poskytování veřejně dostupných informačních služeb o účastnických číslech a účastnických seznamů; souhlas účastníka; rozlišování podle členského státu, v němž jsou veřejně dostupné informační služby o účastnických číslech a účastnické seznamy poskytovány]

Spojené věci C-203/15 a C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen a Secretary of State for the Home Department v. Tom Watson a další*, velký senát, 21. prosince 2016
[Důvěrnost elektronických komunikací; poskytovatelé služeb elektronických komunikací; povinnost plošného a nediferencovaného uchovávání provozních a lokačních údajů; neexistence předchozího přezkumu ze strany soudu nebo nezávislého správního orgánu; Listina základních práv Evropské unie; slučitelnost s právem EU]



Rejstřík

Judikatura Soudního dvora Evropské unie

Judikatura Evropského soudu pro lidská práva

Judikatura vnitrostátních soudů

Mnoho informací o Agentuře Evropské unie pro základní práva je k dispozici na internetu. Lze je nalézt na webových stránkách agentury FRA na adrese fra.europa.eu.

Další informace o judikatuře Evropského soudu pro lidská práva jsou dostupné na webových stránkách soudu: echr.coe.int. Vyhledávací portál HUDOC umožňuje přístup k rozsudkům a rozhodnutím v angličtině a/nebo ve francouzštině, překladům do dalších jazyků, stručným informacím o projednávaných případech, tiskovým zprávám a dalším informacím o práci soudu.

Jak získat publikace Rady Evropy

Nakladatelství Rady Evropy vydává publikace týkající se veškerých aktivit organizace, k nimž patří lidská práva, právní věda, zdraví, etika, sociální věci, životní prostředí, vzdělávání, kultura, sport, mládež a architektonické dědictví. Knihy a elektronické publikace uvedené v obsáhlém katalogu se mohou objednat na webových stránkách (http://book.coe.int/).

Virtuální čítárna umožňuje návštěvníkům zdarma konzultovat výňatky z hlavních čerstvě vydaných publikací či úplné texty určitých oficiálních dokumentů.

Informace o úmluvách Rady Evropy a jejich úplné znění jsou k dispozici na stránkách Oddělení smluv: http://conventions.coe.int/.

Obraťte se na EU

Osobně

Po celé Evropské unii se nachází stovky informačních středisek Europe Direct. Adresu nejbližšího střediska naleznete na internetové stránce: https://europa.eu/european-union/contact_cs.

Telefonicky nebo e-mailem

Europe Direct je služba, která odpoví na vaše dotazy o Evropské unii. Můžete se na ni obrátit:
— prostřednictvím bezplatné telefonní linky: 00 800 6 7 8 9 10 11 (někteří operátoři mohou tento hovor účtovat),
— na standardním telefonním čísle: +32 22999696 nebo
— e-mailem prostřednictvím internetové stránky: https://europa.eu/european-union/contact_cs.

Vyhledávání informací o EU

On-line

Informace o Evropské unii ve všech úředních jazycích EU jsou dostupné na internetových stránkách Europa na adrese: https://europa.eu/european-union/index_cs.

Publikace EU

Publikace EU, ať už bezplatné, nebo placené, si můžete stáhnout nebo objednat na adrese: https://op.europa.eu/cs/publications. Chcete-li obdržet více než jeden výtisk bezplatných publikací, obraťte se na službu Europe Direct nebo na místní informační střediska (viz https://europa.eu/european-union/contact_cs).

Právo EU a související dokumenty

Právní informace EU včetně všech právních předpisů EU od roku 1952 ve všech úředních jazykových verzích jsou dostupné na stránkách EUR-Lex na adrese: http://eur-lex.europa.eu.

Veřejně přístupná data od EU

Portál veřejně přístupných dat EU (http://data.europa.eu/euodp/cs) umožňuje přístup k datovým souborům z EU. Data lze bezplatně stahovat a opakovaně použít pro komerční i nekomerční účely.

doi:10.2811/28452 TK-05-17-225-CS-N

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

EDPS

Rychlý vývoj informací a komunikačních technologií zdůrazňuje rostoucí potřebu spolehlivé ochrany osobních údajů – práva, jež zaručují jak nástroje Evropské unie (EU), tak nástroje Rady Evropy (RE). Ochrana tohoto důležitého práva přináší nové a významné výzvy, jelikož technologický pokrok rozšiřuje hranice oblastí, jako je dozor, odposlouchávání komunikací a uchovávání údajů. Tato příručka je určena k tomu, aby právníky, kteří se nespecializují na oblast ochrany údajů, s touto oblastí práva seznámila. Poskytuje přehled platných právních rámců EU a RE. Vysvětluje rovněž klíčovou judikaturu, shrnuje hlavní rozhodnutí Evropského soudu pro lidská práva i Soudního dvora Evropské unie. Kromě toho představuje hypotetické scénáře, které slouží jako praktické ilustrace rozmanitých problémů, s nimiž se v tomto neustále se měnícím oboru potýkáme.

AGENTURA EVROPSKÉ UNIE PRO ZÁKLADNÍ PRÁVA
Schwarzenbergplatz 11 – 1040 Vídeň – Rakousko
Tel. +43 (1) 580 30-0 – Fax +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA
RADA EVROPY
67075 Strasbourg Cedex – Francie
Tel. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ
Rue Wiertz 60 – 1047 Brusel – Belgie
Tel. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS

Úřad pro publikace Evropské unie
ISBN 978-92-871-9816-7 (RE)
ISBN 978-92-9474-444-9 (FRA)