PŘÍRUČKA

# Příručka evropského práva v oblasti ochrany údajů

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Rukopis této příručky byl dokončen v dubnu 2014.
Aktualizace budou v budoucnu k dispozici na internetových stránkách agentury FRA na adrese: fra.europa.eu, na internetových stránkách Rady Evropy na adrese www.coe.int/dataprotection a na internetových stránkách Evropského soudu pro lidská práva pod nabídkou *Case-Law* [judikatura] na adrese: www.echr.coe.int.



***Europe Direct je služba, která vám pomůže odpovědět na otázky týkající se Evropské unie.***

**Bezplatná telefonní linka** (*):
**00 800 6 7 8 9 10 11**

(*) Informace jsou poskytovány zdarma, stejně jako většina telefonních hovorů (někteří operátoři, telefonní automaty nebo hotely však mohou telefonické spojení zpoplatnit).

Foto (obálka a vnitřek): © iStockphoto

Mnoho doplňujících informací o Evropské unii je k dispozici na internetu.
Můžete se s nimi seznámit na portálu Europa (http://europa.eu).

Lucemburk: Úřad pro publikace Evropské unie, 2015

ISBN 978-92-871-9933-1 (Rada Evropy)
ISBN 978-92-9239-326-7 (FRA)
doi:10.2811/53430

*Printed in Belgium*

Vytištěno na recyklovaném papíře bez použití chloru (PCF)




# Příručka evropského práva v oblasti ochrany údajů

# Předmluva

Tuto příručku evropského práva v oblasti ochrany údajů vypracovaly Agentura Evropské unie pro základní práva (dále jen „FRA") a Rada Evropy ve spolupráci s Kanceláří Evropského soudu pro lidská práva. Jedná se o třetí příručku ze série právních příruček vypracovaných agenturou FRA a Radou Evropy. V březnu 2011 byla vydána první příručka zaměřená na evropské antidiskriminační právo a v červnu 2013 byla vydána druhá zaměřená na evropské právo v oblasti azylu, hranic a přistěhovalectví.

Rozhodli jsme se v naší spolupráci pokračovat na vysoce aktuální téma, které každý den ovlivňuje každého z nás, a sice ochrana osobních údajů. Evropa má v této oblasti jeden z nejúčinnějších ochranných systémů, který je založen na Úmluvě Rady Evropy č. 108, nástrojích Evropské unie (EU) i judikatuře Evropského soudu pro lidská práva (ESLP) a Soudního dvora Evropské unie.

Cílem této příručky je zvýšit povědomí a zlepšit znalosti ohledně pravidel ochrany údajů v Evropské unii a členských státech Rady Evropy tím, že čtenářům poskytne hlavní referenční materiál, do něhož mohou nahlížet. Je určena nespecializovaným právníkům, soudcům, vnitrostátním orgánům pro ochranu údajů a dalším osobám pracujícím v oblasti ochrany údajů.

Vstupem Lisabonské smlouvy v platnost v prosinci 2009 se stala Listina základních práv EU právně závaznou a právo na ochranu osobních údajů tím bylo povýšeno na samostatné základní právo. Lepší porozumění Úmluvě Rady Evropy č. 108 a nástrojům EU, které připravily cestu pro ochranu údajů v Evropě, i judikatuře Soudního dvora a ESLP je zásadní pro ochranu tohoto základního práva.

Rádi bychom poděkovali Institutu Ludwiga Boltzmanna pro lidská práva za přispění při přípravě této příručky. Rovněž bychom chtěli vyjádřit vděčnost úřadu evropského inspektora ochrany údajů za zpětnou vazbu během přípravné fáze. Děkujeme zejména útvaru ochrany údajů Evropské komise za úsilí při přípravě této příručky. Rádi bychom take vyjádřili dík paní Haně Štěpánkové za revizi překladu do češtiny.

**Philippe Boillat**

generální ředitel pro
lidská práva a právní stat
Rada Evropy

**Morten Kjaerum**

ředitel Agentury
Evropské unie
pro základní práva

# Obsah

# Zkratky a akronymy

| | |
|---|---|
| **CCTV** | Kamerový systém |
| **CETS** | Řada smluv Rady Evropy |
| **CIS** | Celní informační systém |
| **CRM** | Řízení zákaznických vztahů |
| **C-SIS** | Centrální schengenský informační systém |
| **EIOÚ** | Evropský inspektor ochrany údajů |
| **ENISA** | Evropská agentura pro bezpečnost sítí a informací |
| **ENU** | Europol National Unit (národní jednotka Europolu) |
| **ES** | Evropské společenství |
| **ESLP** | Evropský soud pro lidská práva |
| **ESMA** | Evropský orgán pro cenné papíry a trhy |
| **ESVO** | Evropské sdružení volného obchodu |
| **eTEN** | Transevropské telekomunikační sítě |
| **EU** | Evropská unie |
| **EuroPriSe** | Evropský systém osvědčení o ochraně soukromí |
| **eu-LISA** | Agentura EU pro rozsáhlé informační systémy |
| **EÚLP** | Evropská úmluva o lidských právech |
| **EZR** | Evropský zatýkací rozkaz, evropský zatykač |
| **FRA** | Agentura Evropské unie pro základní práva |
| **GPS** | Globální systém pro určování polohy |
| **JSB** | Společný dozorový orgán |
| **Listina** | Listina základních práv Evropské unie |
| **NGO** | Nevládní organizace |
| **N-SIS** | Národní součást SIS (schengenského systému) |
| **OECD** | Organizace pro hospodářskou spolupráci a rozvoj |

| | |
|---|---|
| **OSN** | Organizace spojených národů |
| **PIN** | Osobní identifikační číslo |
| **PNR** | Jmenná evidence cestujících |
| **RE** | Rada Evropy |
| **SEPA** | Jednotná oblast pro platby v eurech |
| **SEU** | Smlouva o Evropské unii |
| **SFEU** | Smlouva o fungování Evropské unie |
| **SIS** | Schengenský informační systém |
| **Soudní dvůr** | Soudní dvůr Evropské unie (do prosince 2009 byl nazýván Soudní dvůr Evropských společenství) |
| **SWIFT** | Society for Worldwide Interbank Financial Telecommunication (Společnost pro celosvětovou mezibankovní finanční komunikaci) |
| **UDHR** | Všeobecná deklarace lidských práv |
| **Úmluva č. 108** | Úmluva o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů (Rada Evropy) |
| **VIS** | Vízový informační systém |
| **ZPP** | Závazné podnikové pravidlo |

# Jak používat tuto příručku

Tato příručka poskytuje přehled rozhodného práva ve věcech ochrany údajů v souvislosti s Evropskou unií (EU) a Radou Evropy (RE).

Příručka slouží jako pomůcka pro právníky, kteří se nespecializují na oblast ochrany údajů; je určena pro advokáty, soudce a ostatní uživatele i pro pracovníky jiných orgánů, včetně nevládních organizací (NGO), kteří se mohou setkat s právními otázkami týkajícími se ochrany údajů.

Jedná se o výchozí referenční materiál týkající se jak práva EU, tak Evropské úmluvy o lidských právech (EÚLP) o ochraně údajů, který objasňuje, jak tuto oblast upravuje právo EU, EÚLP i Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů (dále jen „úmluva č. 108“) a další nástroje RE. V každé kapitole je nejprve uvedena tabulka platných právních předpisů, včetně důležité vybrané judikatury podle těchto dvou samostatných evropských právních systémů. Poté jsou postupně představeny příslušné právní předpisy těchto dvou evropských řádů, které se vztahují ke každému tématu. Tak čtenář vidí, kde se tyto dva právní systémy sbíhají a kde se liší.

Tabulky na začátku každé kapitoly poskytují přehled témat probíraných v dané kapitole, uvádějí platné právní předpisy a další relevantní materiály, jako je judikatura. Pořadí témat se může mírně lišit od toho, jak je text kapitoly strukturován, je-li to považováno za vhodné z hlediska stručného přehledu obsahu kapitoly. Tabulky zahrnují jak právo RE, tak EU. To by uživatelům mělo pomoci najít důležité informace týkající se jejich situace, zejména pokud podléhají pouze právu RE.

Uživatelé ze států, jež nejsou členy EU, ale jsou členskými státy RE a stranami EÚLP a úmluvy č. 108, mohou najít informace týkající se jejich vlastní země, když se podívají přímo do oddílů o RE. Uživatelé z členských států EU musí používat oba oddíly, jelikož tyto státy jsou vázány oběma právními řády. Ti, kteří chtějí získat více informací o konkrétní otázce, najdou seznam odkazů na specializovanější materiály v oddílu „Další literatura“ této příručky.

Právo RE je představováno formou stručných odkazů na věci Evropského soudu pro lidská práva (ESLP), které byly vybrané z velkého množství rozsudků a rozhodnutí ESLP, jež lze na téma ochrany údajů najít.

Právo EU je uvedeno v přijatých legislativních opatřeních, v příslušných ustanoveních smluv a Listiny základních práv Evropské unie vykládaných v judikatuře Soudního dvora Evropské unie (dále jen „Soudní dvůr“, před rokem 2009 uváděn jako Soudní dvůr Evropských společenství).

Judikatura popisovaná nebo citovaná v této příručce poskytuje příklady z významného souboru judikatury ESLP i Soudního dvora. Pokyny na konci této příručky mají čtenáři pomoci při vyhledávání judikatury na internetu.

V rámečcích s modrým pozadím jsou dále uvedeny praktické příklady s hypotetickými scénáři pro podrobnější objasnění používání pravidel pro ochranu údajů v praxi, zejména pokud k danému tématu neexistuje žádná konkrétní judikatura ESLP nebo Soudního dvora. V dalších rámečcích se šedým pozadím jsou uvedeny příklady převzaté z jiných zdrojů než z judikatury, např. z právních předpisů.

Příručka začíná stručným popisem úlohy těchto dvou právních systémů ustavených EÚLP nebo právem EU (kapitola 1). Kapitoly 2 až 8 se zabývají těmito tématy:

- terminologie ochrany údajů,
- základní zásady evropského práva v oblasti ochrany údajů,
- pravidla evropského práva v oblasti ochrany údajů,
- práva subjektů údajů a jejich prosazování,
- předávání údajů do zahraničí,
- ochrana údajů v kontextu práce policie a trestního soudnictví,
- další specifické evropské právní předpisy v oblasti ochrany údajů.

# 1

# Kontext a souvislosti evropského práva ochrany údajů

| EU | Probíraná témata | RE |
|---|---|---|
| **Právo na ochranu 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 | | Článek 8 EÚLP (právo na respektování soukromého a rodinného života, obydlí a korespondence)<br>Úmluva o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů (úmluva č. 108) |
| **Vyvažování práv** | | |
| Rozsudek Soudního dvora ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen,* 2010 | **Obecně** | |
| Rozsudek Soudního dvora, C-73/07, *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy a Satamedia Oy,* 2008 | **Svoboda projevu** | Rozsudek ESLP, *Axel Springer AG proti Německu,* 2012<br>Rozsudek ESLP, *Mosley proti Spojenému království*, 2011 |
| | **Svoboda umění a věd** | Rozsudek ESLP, *Vereinigung bildender Künstler proti Rakousku,* 2007 |
| Rozsudek Soudního dvora, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU,* 2008 | **Ochrana vlastnictví** | |
| Rozsudek Soudního dvora, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd,* 2010 | **Přístup k dokumentům** | Rozsudek ESLP, *Társaság a Szabadságjogokért proti Maďarsku,* 2009 |

# 1.1. Právo na ochranu údajů

## Hlavní body

- V souladu s článkem 8 EÚLP je právo na ochranu proti shromažďování a používání osobních údajů součástí práva na respektování soukromého a rodinného života, obydlí a korespondence.
- Úmluva RE č. 108 je prvním mezinárodně právně závazným nástrojem, který se ochranou údajů výslovně zabývá.
- Podle práva EU jako první upravovala ochranu údajů směrnice o ochraně údajů.
- Podle práva EU byla ochrana údajů uznána jako základní právo.

Právo na ochranu soukromé sféry jednotlivce před narušením ze strany druhých, zejména ze strany státu, bylo poprvé stanoveno v mezinárodním právním nástroji v článku 12 Všeobecné deklarace lidských práv Organizace spojených národů (OSN) z roku 1948 o respektování soukromého a rodinného života.[1] Všeobecná deklarace lidských práv ovlivnila vývoj dalších nástrojů týkajících se lidských práv v Evropě.

## 1.1.1. Evropská úmluva o lidských právech

Rada Evropy byla založena po druhé světové válce s cílem sjednotit státy Evropy a podporovat právní stát, demokracii, lidská práva a sociální rozvoj. Za tímto účelem v roce 1950 přijala Evropskou úmluvu o lidských právech (EÚLP), která vstoupila v platnost v roce 1953.

Státy jsou vázány mezinárodní povinností dodržovat EÚLP. Všechny členské státy RE již EÚLP začlenily nebo provedly ve svém vnitrostátním právu, které vyžaduje, aby jednaly v souladu s ustanoveními této úmluvy.

Aby bylo zajištěno, že smluvní strany dodržují své povinnosti v souladu s EÚLP, byl v roce 1959 ve Štrasburku zřízen Evropský soud pro lidská práva (ESLP). ESLP zajišťuje, aby státy dodržovaly své povinnosti v souladu s úmluvou č.108 tak, že se zabývá stížnostmi jednotlivců, skupin jednotlivců, nevládních organizací nebo právnických subjektů na porušení úmluvy. V roce 2013 Rada Evropy zahrnovala 47 členských států, z nichž 28 je rovněž členskými státy EU. Stěžovatelem v řízení před ESLP

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

nemusí být občan jednoho z členských států. ESLP se může zabývat také mezistátními věcmi předloženými jedním či více členskými státy RE proti jinému členskému státu.

Právo na ochranu osobních údajů je součástí práv chráněných podle článku 8 EÚLP, který zaručuje právo na respektování soukromého a rodinného života, obydlí a korespondence a stanoví podmínky, za nichž se povoluje omezování tohoto práva.[2]

V rámci své judikatury se ESLP již zabýval mnoha situacemi, v nichž figurovala otázka ochrany údajů, a to i otázkami týkajícími se sledování komunikace,[3] různých forem dohledu[4] a ochrany před uchováváním osobních údajů veřejnými orgány.[5] Objasnil, že článek 8 EÚLP nejenom státům ukládá, aby se zdržely jednání, které by mohlo právo stanovené úmluvou č.108 porušovat, ale aby byly v určitých situacích rovněž povinny aktivně zabezpečovat účinné respektování soukromého a rodinného života.[6] Mnohé z těchto věcí budou podrobně uvedeny v příslušných kapitolách.

## 1.1.2. Úmluva Rady Evropy č. 108

S rozmachem informačních technologií v šedesátých letech dvacátého století se rozvinula rostoucí potřeba podrobnějších pravidel pro ochranu jednotlivců prostřednictvím ochrany jejich (osobních) údajů. Do poloviny sedmdesátých let dvacátého století Výbor ministrů Rady Evropy přijal řadu usnesení o ochraně osobních údajů, v nichž odkazoval na článek 8 EÚLP.[7] V roce 1981 byla otevřena k podpisu Úmluva o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů

2 RE, Evropská úmluva o lidských právech, CETS č. 005, 1950.

3 Viz například: Rozsudek ESLP ze dne 2. srpna 1984, *Malone proti Spojenému království*, č. 8691/79; rozsudek ESLP ze dne 3. dubna 2007, *Copland proti Spojenému království*, č. 62617/00.

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

5 Viz například: Rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81; rozsudek ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04.

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

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

(úmluva č. 108)[8]. Úmluva č. 108 byla a stále zůstává jediným právně závazným mezinárodním nástrojem v oblasti ochrany údajů.

Úmluva č. 108 se použije na veškeré zpracování údajů prováděné jak soukromým, tak veřejným sektorem, jako je zpracování údajů justičními a donucovacími orgány. Chrání jednotlivce před zneužíváním, které může doprovázet shromažďování a zpracování osobních údajů, a zároveň usiluje o regulaci předávání údajů do zahraničí. Pokud jde o shromažďování a zpracování osobních údajů, zásady stanovené v úmluvě č.108 se týkají zejména korektního a zákonného shromažďování a automatizovaného zpracování údajů, které jsou uchovávány pro specifikované zákonné účely a nikoli pro potřeby neslučitelné s těmito účely a které rovněž nejsou uchovávány po delší dobu, než je nezbytné. Týkají se též kvality údajů, zejména toho, že musejí být přiměřené, podstatné, rozsahem nezbytné pro naplnění účeli (proporcionalita) a přesné.

Kromě poskytování záruk pro shromažďování a zpracování osobních údajů úmluva č. 108 zakazuje v případě neexistence řádných právních ochranných opatření zpracování „citlivých" údajů, jako jsou údaje o rase, politickém smýšlení, zdravotním stavu, náboženském vyznání, sexuálním životě nebo záznamu v trestním rejstříku určité osoby.

Úmluva č. 108 rovněž stanoví právo jednotlivce být informován o tom, jaké informace jsou o něm uchovávány, a právo na jejich opravu v případě potřeby. Omezení práv stanovených úmluvou jsou možná pouze v případě vyšších zájmů, jako je bezpečnost nebo obrana státu.

Přestože úmluva č. 108 umožňuje volné předávání osobních údajů mezi státy, jež jsou stranami úmluvy, rovněž ukládá několik omezení tohoto předávání do států, kde právní předpisy nezajišťují ekvivalentní ochranu.

V zájmu dalšího rozvíjení obecných zásad a pravidel stanovených v úmluvě č. 108 Výbor ministrů RE přijal několik doporučení, která nejsou právně závazná (viz kapitola 7 a 8).

8 RE, Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů, CETS č. 108, 1981.

Úmluvu č. 108 ratifikovaly všechny členské státy EU. V roce 1999 byla úmluva č. 108 změněna, aby se stranou mohla stát EU.[9] V roce 2001 byl přijat dodatkový protokol k úmluvě č. 108, který zavedl ustanovení o předávání údajů do zahraničí takzvaným třetím zemím, které nejsou stranami úmluvy, a o povinném zřízení vnitrostátních orgánů dozoru pro ochranu údajů.[10]

### Výhled

Poté, co bylo přijato rozhodnutí modernizovat úmluvu č. 108, uskutečnily se v roce 2011 veřejné konzultace, díky nimž bylo možné potvrdit dva hlavní cíle dané práce: zvýšit ochranu soukromí v digitální oblasti a posílit návazný mechanismus úmluvy.

Úmluva č. 108 je otevřena k přistoupení nečlenským státům RE, včetně mimoevropských zemí. Potenciál úmluvy jakožto univerzální normy a její otevřený charakter by mohly být základem pro podporu ochrany údajů na světové úrovni.

Zatím 45 ze 46 smluvních stran úmluvy č. 108 jsou členské státy RE. Uruguay, první mimoevropská země, přistoupila v srpnu 2013, a Maroko, které k přistoupení k úmluvě č. 108 vyzval Výbor ministrů, se nachází ve fázi formalizace přistoupení.

## 1.1.3. Evropské právo v oblasti ochrany údajů

Právo EU se skládá ze smluv a sekundárního práva EU. Smlouvy, jmenovitě Smlouva o Evropské unii (SEU) a Smlouva o fungování Evropské unie (SFEU), byly schváleny všemi členskými státy EU a označují se též jako „primární právo EU". Nařízení, směrnice a rozhodnutí EU přijímají orgány EU, jež k tomu byly zmocněny smlouvami, a často se označují jako „sekundární právo EU".

Základním právním nástrojem EU v oblasti ochrany osobních údajů je 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*).[11] Byla přijata v roce 1995, v době, kdy již několik členských států přijalo vnitrostátní právní předpisy o ochraně osobních údajů. Volný

9 RE, Změny Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracovávání osobních údajů (CETS č. 108) zakládající možnost Evropských společenství přistoupit, které přijal Výbor ministrů Rady Evropy ve Štrasburku dne 15. června 1999; čl. 23 odst. 2 Úmluvy č. 108 v pozměněném znění.

10 RE, Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních údajů, o orgánech dozoru a toku údajů přes hranice, CETS č. 181, 2001.

11 Směrnice o ochraně údajů, Úř. věst. 1995 L 281, s. 31.

pohyb zboží, kapitálu, služeb a osob na vnitřním trhu vyžadoval volný pohyb údajů, jež by nebylo možné realizovat, pokud by se členské státy nemohly spolehnout na jednotnou vysokou úroveň ochrany osobních údajů.

Jelikož cílem přijetí směrnice o ochraně údajů byla harmonizace[12] právních předpisů o ochraně údajů na vnitrostátní úrovni, umožňuje tato směrnice určitou míru specifičnosti srovnatelnou s mírou specifičnosti (tehdejších) vnitrostátních právních předpisů o ochraně údajů. Podle Soudního dvora „cílem směrnice 95/46 […] je dosáhnout ve všech členských státech rovnocenné úrovně ochrany práv a svobod osob v souvislosti se zpracováním osobních údajů. […] Sblížení vnitrostátních právních předpisů použitelných v dané oblasti nesmí vést k oslabení ochrany, kterou zajišťují, ale musí mít naopak za cíl zajištění vysoké úrovně ochrany v Unii. […] Harmonizace uvedených vnitrostátních právních předpisů se neomezuje na minimální harmonizaci, ale vede k zásadně úplné harmonizaci.“[13] Členské státy mají tudíž při provádění směrnice pouze omezený manévrovací prostor.

Účelem směrnice o ochraně údajů je konkretizovat zásady práva na soukromí, které jsou již uvedené v úmluvě č. 108, a rozšířit je. Skutečnost, že všech 15 členských států EU v roce 1995 bylo též smluvními stranami úmluvy č. 108, vylučuje přijetí protichůdných pravidel v těchto dvou právních nástrojích. Směrnice o ochraně údajů nicméně využívá možnosti stanovené v článku 11 úmluvy č. 108 přidávat nástroje ochrany. Zejména zavedení nezávislého dozoru jako nástroje pro zlepšení dodržování pravidel týkajících se ochrany údajů se ukázalo jako důležité přispění k účinnému fungování evropského práva v oblasti ochrany údajů. (Tento prvek byl poté v roce 2001 přejat do práva RE prostřednictvím dodatkového protokolu k úmluvě č. 108).

Územní uplatňování směrnice o ochraně údajů se rozšiřuje za 28 členských států, včetně mimoevropských členských států, které jsou součástí Evropského hospodářského prostoru (EHP)[14] – jmenovitě Island, Lichtenštejnsko a Norsko.

Pravomoc stanovovat, zda členský stát plní své povinnosti podle směrnice o ochraně údajů, a rozhodovat o předběžných otázkách týkajících se platnosti

12 Viz např. 1, 4., 7. a 8. bod odůvodnění směrnice o ochraně údajů.

13 Rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, body 28–29.

14 Dohoda o Evropském hospodářském prostoru, Úř. věst. 1994 L 1, jež vstoupila v platnost dne 1. ledna 1994.

a výkladu této směrnice pro zajištění jejího účinného a jednotného uplatňování v členských státech, má Soudní dvůr v Lucemburku. Důležitou výjimkou z uplatňování směrnice o ochraně údajů je takzvaná výjimka týkající se zpracování údajů pro osobní potřebu, tedy zpracování osobních údajů soukromými osobami pouze pro osobní či domácí účely.[15] Takové zpracování je obecně vnímáno jako součást svobod soukromé osoby.

Vzhledem k primárnímu právu EU, jež bylo v platnosti v okamžiku přijetí směrnice o ochraně údajů, se věcná působnost směrnice omezuje na záležitosti vnitřního trhu. Do její působnosti nespadají zejména záležitosti spolupráce policie a trestního soudnictví. Ochranu údajů v těchto záležitostech zajišťují různé právní nástroje, které jsou podrobně popsány v kapitole 7.

Jelikož směrnice o ochraně údajů se mohla týkat pouze členských států EU, byl zapotřebí další právní nástroj, jenž by stanovil ochranu údajů pro zpracování osobních údajů institucemi a orgány EU. Tento úkol splňuje 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 zpracovávaných institucemi EU*).[16]

Navíc i v oblastech, jimiž se zabývá směrnice o ochraně údajů, jsou často zapotřebí podrobnější ustanovení o ochraně údajů, aby bylo dosaženo nezbytné jasnosti při zajišťování rovnováhy s ostatními oprávněnými zájmy. Dvěma příklady jsou směrnice 2002/58/ES o zpracovávání osobních údajů a ochraně soukromí v odvětví elektronických komunikací (*směrnice o soukromí a elektronických komunikacích*)[17] a směrnice 2006/24/ES 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 *(směrnice o uchovávání údajů,* která byla prohlášena za neplatnou dne 8. dubna 2014).[18]

15 2. odrážka čl. 3 odst. 2 směrnice o ochraně údajů.

16 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.

17 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.

18 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, (směrnice o uchovávání údajů), Úř. věst. 2006 L 105, prohlášena za neplatnou dne 8. dubna 2014.

Dalším příkladům se věnuje kapitola 8. Tato ustanovení musí být v souladu se směrnicí o ochraně údajů.

## Listina základních práv Evropské unie

V původních smlouvách Evropských společenství nebyly žádné zmínky o lidských právech nebo jejich ochraně. Jelikož se však k tehdejšímu Soudnímu dvoru Evropských společenství dostaly případy, v nichž byla vznesena obvinění z porušování lidských práv v oblastech spadajících do působnosti práva EU, Soudní dvůr rozvinul nový přístup. Aby zajistil ochranu jednotlivcům, přidal základní práva mezi takzvané obecné zásady evropského práva. Podle Soudního dvora tyto obecné zásady odrážejí obsah ochrany lidských práv ve vnitrostátních ústavách a smlouvách o lidských právech, zejména EÚLP. Soudní dvůr prohlásil, že bude zajišťovat shodu práva EU s těmito zásadami.

Jelikož EU si uvědomovala, že její zásady by mohly mít dopad na lidská práva, a ve snaze zajistit, aby se občané cítili „blíže" EU, v roce 2000 vyhlásila Listinu základních práv Evropské unie (dále jen „Listina"). Tato Listina zahrnuje celou řadu občanských, politických, ekonomických a sociálních práv evropských občanů na základě sloučení ústavních tradic a mezinárodních povinností společných členským státům. Práva popisovaná v Listině jsou rozdělena do šesti oddílů: důstojnost, svobody, rovnost, solidarita, občanská práva a soudnictví.

Přestože Listina byla původně pouze politickým dokumentem, stala se právně závaznou[19] jako primární právo EU (viz čl. 6 odst. 1 SEU) od 1. prosince 2009, kdy vstoupila v platnost Lisabonská smlouva.[20]

Primární právo EU též zahrnuje celkovou způsobilost EU přijímat právní předpisy v záležitostech ochrany údajů (článek 16 SFEU).

Listina nejen zaručuje respektování soukromého a rodinného života (článek 7), ale také stanoví právo na ochranu údajů (článek 8), přičemž výslovně povyšuje úroveň této ochrany na úroveň základního práva v právu EU. Orgány EU i členské státy musí dodržovat a zaručit toto právo, jež se použije též pro členské státy při uplatňování práva Unie (článek 51 Listiny). Listina byla sepsána několik let po směrnici

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

20 Viz konsolidovaná znění Smlouvy o Evropské unii, Evropská společenství (2012), Úř. věst. 2012 C 326; a SFEU, Evropská společenství (2012), Úř. věst. 2012 C 326.

o ochraně údajů, článek 8 Listiny je však nutno chápat tak, že zahrnuje dřívější právo EU týkající se ochrany údajů. Listina tudíž nejenom výslovně uvádí právo na ochranu údajů v čl. 8 odst. 1, ale také odkazuje na hlavní zásady ochrany údajů v čl. 8 odst. 2. A konečně čl. 8 odst. 3 Listiny z ukládá, že na provádění těchto zásad dohlíží nezávislý orgán.

### Výhled

V lednu 2012 navrhla Evropská komise balíček opatření pro reformu ochrany údajů s tím, že stávající pravidla v oblasti ochrany údajů je třeba modernizovat vzhledem k rychlému technologickému rozvoji a globalizaci. Balíček opatření pro reformu tvoří návrh obecného nařízení o ochraně údajů,[21] které mělo nahradit směrnici o ochraně údajů, i nové obecné směrnice o ochraně údajů,[22] jež měla stanovit ochranu údajů v oblasti spolupráce policie a soudů v trestních věcech. V okamžiku zveřejnění této příručky jednání o reformním balíčku ještě probíhala.

## 1.2. Zajišťování rovnováhy práv

**Hlavní bod**

- Právo na ochranu údajů není absolutní právo; musí být v rovnováze s ostatními právy.

Základní právo na ochranu osobních údajů se podle článku 8 Listiny „však neprojevuje jako absolutní výsada, ale musí k němu být přihlédnuto ve vztahu k jeho funkci ve společnosti“.[23] Čl. 52 odst. 1 Listiny tudíž stanoví, že výkon práv, jako jsou práva ustanovená v článku 7 a 8 Listiny, je možné omezovat, pokud jsou taková omezení ukládána zákonem, respektují podstatu těchto práv a svobod a při dodržení zásady proporcionality, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Evropská unie, nebo potřebě ochrany práv a svobod druhého.[24]

21 Evropská komise (2012), Návrh nařízení Evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), KOM(2012) 11 v konečném znění, Brusel, 25. ledna 2012.

22 Evropská komise (2012), *Návrh 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 (obecná směrnice o ochraně údajů)*, KOM(2012) 10 v konečném znění, Brusel, 25. ledna 2012.

23 Viz např. rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*, bod 48.

24 *Tamtéž*, bod 50.

V systému EÚLP ochranu údajů zaručuje článek 8 (právo na respektování soukromého a rodinného života) a v systému Listiny je potřeba toto právo uplatňovat a zároveň respektovat rozsah ostatních práv, jež si konkurují. V souladu s čl. 8 odst. 2 EÚLP „státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu [...] ochrany práv a svobod jiných".

Proto jak ESLP, tak Soudní dvůr opakovaně prohlašují, že při používání a výkladu článku 8 EÚLP a článku 8 Listiny je nezbytné zajišťovat při výkonu práv rovnováhu s dalšími právy.[25] Na několika významných příkladech si ukážeme, jak lze této rovnováhy dosáhnout.

## 1.2.1. Svoboda projevu

Jedním z práv, u nějž existuje pravděpodobnost, že se dostane do střetu s právem na ochranu osobních údajů, je právo na svobodu projevu.

Svobodu projevu chrání článek 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". Článek 11 odpovídá článku 10 EÚLP. V souladu s čl. 52 odst. 3 Listiny, 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 lze ze zákona uplatňovat na právo zakotvené v článku 11 Listiny, tudíž nesmějí překročit omezení stanovená v čl. 10 odst. 2 EÚLP, to znamená, že musí být stanovena zákonem a musí být nezbytná v demokratické společnosti „v zájmu [...] ochrany pověsti nebo práv jiných". Toto pojetí zahrnuje právo na ochranu osobních údajů.

Vztah mezi ochranou osobních údajů a svobodou projevu upravuje článek 9 směrnice o ochraně údajů s názvem „Zpracování osobních údajů a svoboda projevu".[26] Podle tohoto článku členské státy stanoví řadu odchylek a výjimek v souvislosti

25 Rozsudek ESLP [velkého senátu] ze dne 7. února 2012, *Von Hannover proti Německu (č. 2)*, č. 40660/08 a 60641/08; rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, bod 48; rozsudek Soudního dvora ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, bod 68. Viz rovněž Rada Evropy (2013), judikatura Evropského soudu pro lidská práva týkající se ochrany osobních údajů, judikatura o ochraně údajů (2013), k dispozici na adrese: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

26 Článek 9 směrnice o ochraně údajů.

s ochranou údajů specifikovanou v kapitolách II, IV a VI uvedené směrnice, a tudíž v souvislosti se základním právem na soukromí. Odchylky musí být prováděné výlučně pro účely žurnalistiky nebo uměleckého či literárního projevu, které spadají do rozsahu základního práva na svobodu projevu, pouze pokud jsou nezbytné pro uvedení práva na soukromí do souladu s předpisy upravujícími svobodu projevu.

Příklad: V rámci sporu mezi *Tietosuojavaltuutettu a Satakunnan Markkinapörssi Oy a Satamedia Oy*[27] byl Soudní dvůr požádán o výklad článku 9 směrnice o ochraně údajů a o definování vztahu mezi ochranou údajů a svobodou tisku. Úkolem Soudního dvora bylo prošetřit zpřístupňování daňových údajů společnostmi Markkinapörssi a Satamedia týkajících se přibližně 1,2 milionu fyzických osob, které zákonným způsobem získaly od finských daňových úřadů. Soudní dvůr měl zejména ověřit, zda musí být zpracovávání osobních údajů, které zpřístupnily daňové úřady, za účelem umožnit uživatelům mobilních telefonů přijímat daňové údaje týkající se jiných fyzických osob, považováno za činnost prováděnou výlučně pro účely žurnalistiky. Poté, co Soudní dvůr dospěl k závěru, že činnosti společnosti Satakunnan představovaly „zpracovávání osobních údajů" ve smyslu čl. 3 odst. 1 směrnice o ochraně údajů, pokračoval výkladem článku 9 uvedené směrnice. Soudní dvůr nejprve poukázal na význam, jenž má právo na svobodu projevu v každé demokratické společnosti, a konstatoval, že pojmy související s touto svobodou, jako je žurnalistika, je třeba vykládat široce. Dále poznamenal, 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 se Soudní dvůr domníval, že takové činnosti, jaké prováděly společnosti Markkinapörssi a Satamedia, 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. Soudní dvůr také rozhodl, že tyto činnosti se neomezují na provozovatele sdělovacích prostředků a mohou být spojeny s výdělečným účelem. Avšak posouzení, zda tomu tak v této konkrétní věci bylo, Soudní dvůr ponechal na vnitrostátním soudu.

V otázce uvedení práva na ochranu osobních údajů do souladu s právem na svobodu projevu vydal ESLP několik významných rozsudků.

27 Rozsudek Soudního dvora ze dne 16. prosince 2008, C-73/07, *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy a Satamedia Oy*, body 56, 61 a 62.

Příklad: Ve věci *Axel Springer AG v. Německo*[28] ESLP rozhodl, že zákaz uložený vnitrostátním soudem vlastníkovi deníku, který chtěl uveřejnit článek o zatčení a odsouzení známého herce, porušuje článek 10 EÚLP. ESLP zopakoval kritéria, která v této judikatuře stanovil v souvislosti se zajišťováním rovnováhy mezi právem na svobodu projevu a právem na respektování soukromého života:

- za prvé, zda byla událost, jíž se dotčený zveřejněný článek týkal, událostí obecného zájmu: zatčení a odsouzení osoby bylo veřejnou soudní skutečností, a tudíž záležitostí veřejného zájmu,
- za druhé, zda dotčená osoba byla významnou osobou: dotčená osoba byla hercem dostatečně známým na to, aby mohl být označen za významnou osobu, a
- za třetí, jak byly informace získány a zda byly spolehlivé: informace poskytl úřad státního zastupitelství, a o přesnosti informací publikovaných oběma stranami není sporu.

ESLP tudíž rozhodl, že omezení zveřejnění uložené společnosti nebylo rozumně přiměřené s ohledem na legitimní cíl chránit soukromý život stěžovatele. Soud dospěl k závěru, že došlo k porušení článku 10 EÚLP.

Příklad: Ve věci *Von Hannover proti Německu (č. 2)*[29] ESLP neshledal žádné porušení práva na respektování soukromého života podle článku 8 EÚLP, když monacké princezně Caroline soud odmítl vydat předběžné opatření proti zveřejnění fotografie, na níž byla se svým mužem, pořízené během dovolené na lyžích. Fotografii doprovázel článek, v němž se mimo jiné psalo o špatném zdravotním stavu prince Rainiera. ESLP dospěl k závěru, že vnitrostátní soudy řádně zajistily rovnováhu mezi právem na svobodu projevu vydavatelství a právem stěžovatelky na respektování soukromého života. Označení onemocnění prince Rainiera vnitrostátními soudy za událost současné společnosti nebylo možné považovat za nepřiměřené a ESLP mohl akceptovat, že fotografie posuzovaná s ohledem na daný článek alespoň do určité míry přispěla k debatě obecného zájmu. Soud dospěl k závěru, že nedošlo k porušení článku 8 EÚLP.

28 Rozsudek ESLP [velkého senátu] ze dne 7. února 2012, *Axel Springer AG proti Německu*, č. 39954/08, body 90 a 91.

29 Rozsudek ESLP [velkého senátu] ze dne 7. února 2012, *Von Hannover proti Německu (č. 2)*, č. 40660/08 a 60641/08, body 118 a 124.

Jedním ze zásadních kritérií v judikatuře ESLP ohledně zajištění rovnováhy těchto práv je, zda dotčený projev přispívá k debatě obecného veřejného zájmu.

Příklad: Ve věci *Mosley v. Spojené království*[30] vnitrostátní týdeník uveřejnil intimní fotografie stěžovatele. Stěžovatel poté tvrdil, že došlo k porušení článku 8 EÚLP, jelikož před zveřejněním dotčených fotografií nemohl zažádat o předběžné opatření, protože pro tisk neexistuje žádný požadavek na předběžné oznámení v případě zveřejňování materiálu, který by mohl porušit právo na soukromí jednotlivce. Přestože účely zpřístupňování takového materiálu byly spíše zábavné než vzdělávací, nepochybně těžil z ochrany poskytované článkem 10 EÚLP, která by mohla ustoupit požadavkům článku 8 EÚLP, pokud by informace byly soukromé a intimní povahy a neexistoval by žádný veřejný zájem pro jejich zpřístupňování. Při posuzování omezení, která by mohla působit jako určitá forma cenzury před zveřejněním, je potřeba postupovat obzvlášť obezřetně. Co se týče odrazujícího účinku (tzv. „chilling effect"), který by požadavek na předběžné oznámení mohl mít, pochybností ohledně jeho účinnosti a velkého prostoru pro posuzování v dané oblasti, ESLP dospěl k závěru, že článek 8 nevyžaduje existenci právně závazného požadavku na předběžné oznámení. Soud tudíž dospěl k závěru, že nedošlo k porušení článku 8.

Příklad: Ve věci *Biriuk proti Litvě*[31] se stěžovatelka domáhala náhrady škody od deníku za to, že uveřejnil článek, v němž tvrdil, že je HIV pozitivní. Tuto informaci údajně potvrdil zdravotnický personál místní nemocnice. ESLP se domníval, že dotčený článek nepřispívá k žádné debatě obecného zájmu, a zopakoval, že ochrana osobních údajů, a to i zdravotnické dokumentace, má zásadní význam pro to, aby osoba mohla požívat svého práva na respektování soukromého a rodinného života, které jí zaručuje článek 8 EÚLP. Soud přikládal zvláštní význam skutečnosti, že podle zprávy v deníku zdravotnický personál nemocnice poskytl informace o HIV infekci stěžovatelky, čímž zcela jasně porušil svoji povinnosti zachovávat lékařské tajemství. Stát tudíž stěžovatelce nezajistil právo na respektování jejího soukromého života. Soud dospěl k závěru, že došlo k porušení článku 8.

30 Rozsudek ESLP ze dne 10. května 2011, *Mosley proti Spojenému království*, č. 48009/08, body 129 a 130.

31 Rozsudek ESLP ze dne 25. listopadu 2008, *Biriuk proti Litvě*, č. 23373/03.

## 1.2.2. Přístup k dokumentům

Svoboda informací v souladu s článkem 11 Listiny a článkem 10 EÚLP chrání právo nejenom na rozšiřování, ale také na *přijímání* informací. Stále je patrnější, jak průhlednost vlády je důležitá pro fungování demokratické společnosti. V posledních dvou desetiletích bylo tudíž právo na přístup k dokumentům uchovávaných veřejnými orgány uznáno jako důležité právo každého občana EU a jakékoli fyzické nebo právnické osoby s bydlištěm nebo sídlem v členském státě.

**Podle práva RE** se lze odvolat na zásady stanovené v doporučení o přístupu k úředním dokumentům, které inspirovalo tvůrce Úmluvy o přístupu k úředním dokumentům (úmluva č. 205).[32] **Podle práva EU** právo na přístup k dokumentům zaručuje nařízení 1049/2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (nařízení o přístupu k dokumentům).[33] 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 použitý nosič". V souladu s čl. 52 odst. 2 Listiny je právo na přístup k dokumentům vykonáváno za podmínek a v mezích stanovených v čl. 15 odst. 3 SFEU. Toto právo může kolidovat s právem na ochranu údajů, pokud by přístup k dokumentu odhalil osobní údaje jiných osob. Žádosti o přístup k dokumentům nebo informacím uchovávaným veřejnými orgány může tudíž vyžadovat zajištění rovnováhy s právem na ochranu osobních údajů osob, jejichž údaje jsou v požadovaných dokumentech obsaženy.

Příklad: Ve věci *Evropská komise proti Bavarian Lager*[34] Soudní dvůr definoval rozsah ochrany osobních údajů v souvislosti s přístupem k dokumentům orgánů EU a vztah mezi nařízeními č. 1049/2001 (nařízení o přístupu k dokumentům) a 45/2001 (nařízení o ochraně údajů). Společnost Bavarian Lager, založená v roce 1992, dováží německé lahvové pivo do Spojeného království, především pro výčepy a bary. Setkala se však s potížemi, protože britská legislativa *de facto* zvýhodňovala vnitrostátní výrobce. V reakci na stížnost společnosti Bavarian Lager Evropská komise rozhodla o zahájení řízení proti Spojenému království z důvodu neplnění jeho povinností, na základě něhož bylo Spojené

32 Rada Evropy, Výbor ministrů (2002), Doporučení č. Rec(2002)2 členským státům o přístupu k úředním dokumentům, 21. února 2002; Rada Evropy, Úmluva Rady Evropy o přístupu k úředním dokumentům, CETS č. 205, 18. června 2009. Úmluva ještě nevstoupila v platnost.

33 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.

34 Rozsudek Soudního dvora ze dne 29. června 2010, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd.*, body 60, 63, 76, 78 a 79.

království nuceno změnit sporná ustanovení a sladit je s právem EU. Společnost Bavarian Lager poté požádala Komisi, mezi jinými dokumenty, o kopii zápisu ze zasedání, kterého se zúčastnili zástupci Komise, britských orgánů a *Confédération des Brasseurs du Marché Commun* (CBMC). Komise souhlasila se zpřístupněním určitých dokumentů týkajících se zasedání, avšak znečitelnila pět jmen uvedených v zápisu, jelikož dvě osoby výslovně vznesly námitku proti zveřejnění své identity a s dalšími třemi se Komise nemohla zkontaktovat. Rozhodnutím ze dne 18. března 2004 Komise zamítla novou žádost společnosti Bavarian Lager o zpřístupnění úplného zápisu ze zasedání zejména s odvoláním na ochranu soukromého života uvedených osob, kterou zaručuje nařízení o ochraně údajů. Jelikož společnost Bavarian Lager nebyla s tímto stanoviskem spokojena, podala opravný prostředek k Soudu prvního stupně, který rozhodnutí Komise zrušil rozsudkem ze dne 8. listopadu 2007 (věc T-194/04, *Bavarian Lager proti Komisi*) zejména s přihlédnutím ke skutečnosti, že pouhé uvedení jmen dotčených osob na seznamu účastníků zasedání jakožto zástupce entity nepředstavuje porušení soukromého života a nijak soukromé životy těchto osob neohrožuje.

Na základě odvolání Komise Soudní dvůr zrušil rozsudek Soudu prvního stupně. Soudní dvůr konstatoval, že nařízení o přístupu k dokumentům zavádí „specifický a zesílený systém ochrany osob, jejichž osobní údaje mohou být případně zpřístupňovány veřejnosti“. Podle Soudního dvora, pokud žádost založená na nařízení o přístupu k dokumentům takto usiluje o přístup k dokumentům obsahujícím osobní údaje, ustanovení nařízení o ochraně údajů budou plně použitelná. Soudní dvůr poté dospěl k závěru, že Komise žádost o přístup k úplnému zápisu ze zasedání konaného v říjnu 1996 zamítla právem. Vzhledem k tomu, že pět účastníků uvedeného zasedání neposkytlo souhlas, Komise dostatečně dostála své povinnosti průhlednosti tím, že šířila znění sporného dokumentu s jejich jmény zakrytými.

Podle Soudního dvora 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.

Podle tohoto rozsudku zásah do práva na ochranu údajů s ohledem na přístup k dokumentům vyžaduje konkrétní a oprávněný důvod. Právo na přístup k dokumentům nemůže automaticky zrušit právo na ochranu osobních údajů.[35]

Konkrétním aspektem žádosti o přístup se zabýval ESLP v následujícím rozsudku.

Příklad: Ve věci *Társaság a Szabadságjogokért proti Maďarsku*[36] stěžovatel, nevládní organizace pro lidská práva, požadoval od ústavního soudu přístup k informacím o projednávané věci. Ústavní soud žádost o přístup zamítl bez konzultace se členem parlamentu, který věc soudu předložil, s odůvodněním, že žaloby podané u tohoto soudu mohou být zpřístupněny třetím osobám pouze se souhlasem žalobce. Vnitrostátní soudy toto zamítnutí potvrdily s odůvodněním, že jiné zákonné zájmy, včetně přístupu k veřejným informacím, nemohou být nadřazeny ochraně takových osobních údajů. Stěžovatel jednal jako „sociální hlídací pes", jehož činnosti zaručovaly podobnou ochranu jako činnosti tisku. V souvislosti se svobodou tisku ESLP trvale zastává názor, že veřejnost má právo na informace obecného zájmu. Informace, jež požadoval stěžovatel, byly *„ready and available"* [připravené a dostupné] a nevyžadovaly shromažďování údajů. Za takových okolností byl stát povinen nebránit předávání informací požadovanému stěžovatelem. Souhrnně řečeno, ESLP se domníval, že překážky, jejichž účelem je zamezit přístupu k informacím veřejného zájmu, mohou odradit pracovníky v oblasti sdělovacích prostředků nebo v souvisejících oblastech od plnění jejich důležité úlohy „ hlídacího psa veřejnosti". Soud dospěl k závěru, že došlo k porušení článku 10.

**Podle práva EU** je význam průhlednosti pevně stanoven. Zásada průhlednosti je zakotvena v článcích 1 a 10 SEU a v čl. 15 odst. 1 SFEU.[37] Podle 2. bodu odůvodnění nařízení (ES) č. 1049/2001 umožňuje občanům blíže se účastnit rozhodovacího

35 Viz však podrobný výklad evropského inspektora ochrany údajů (EIOÚ) (2011), *Veřejný přístup k dokumentům, které obsahují osobní údaje, poté, co byl vydán rozsudek ve věci* Bavarian Lager, Brusel, 24. března 2011, k dispozici na adrese: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 Rozsudek ESLP ze dne 14. dubna 2009, *Társaság a Szabadságjogokért proti Maďarsku*, č. 37374/05; viz body 27, 36–38.

37 EU (2012), konsolidovaná znění Smlouvy o Evropské unii a SFEU, Úř. věst. 2012 C 326.

procesu a zaručuje, že správní orgány budou mít ve vztahu k občanům v demokratickém systému větší legitimitu, účinnost a odpovědnost.[38]

Z tohoto důvodu nařízení Rady (ES) č. 1290/2005 o financování společné zemědělské politiky a nařízení Komise (ES) č. 259/2008, kterým se stanoví prováděcí pravidla k tomuto nařízení, vyžadují zveřejňování informací o příjemcích finančních prostředků určitých fondů EU v odvětví zemědělství a o částkách přijatých jednotlivými příjemci.[39] Zveřejňování by mělo přispět k veřejné kontrole nad vhodným využíváním veřejných finančních prostředků správními orgány. Několik příjemců napadlo proporcionalitu tohoto zveřejňování.

Příklad: Ve věci *Volker und Markus Schecke a Hartmut Eifert proti Land Hessen*[40] musel Soudní dvůr posoudit proporcionalitu zveřejňování jména příjemců zemědělských dotací EU a přijatých částek, jež vyžadují právní předpisy EU.

S tím, že ochrana údajů není absolutní, Soudní dvůr uvedl, že zveřejnění jmenovitých údajů o příjemcích a přesných částkách, které obdrželi, na internetové stránce obecně představuje zásah do práva dotčených příjemců na respektování jejich soukromého života obecně a konkrétně na ochranu jejich osobních údajů.

Soudní dvůr se domníval, že takový zásah do práv zakotvených v článcích 7 a 8 Listiny je stanoven zákonem a odpovídá cíli obecného zájmu uznávanému EU, jmenovitě zvýšení průhlednosti využívání finančních prostředků Společenství. Soudní dvůr však rozhodl, že zveřejnění jmen fyzických osob, které jsou příjemci podpory EU v zemědělství z těchto dvou fondů, a přesných částek, které obdržely, představuje nepřiměřené opatření a není odůvodněné s ohledem na čl. 52 odst. 1 Listiny. Soudní dvůr tudíž prohlásil právní předpisy týkající se

38 Rozsudek Soudního dvora ze dne 6. března 2003, C-41/00 P, *Interporc Im- und Export GmbH proti Komisi Evropských společenství*, bod 39; a rozsudek Soudního dvora ze dne 29. června 2010, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd.*, bod 54.

39 Nařízení Rady (ES) č. 1290/2005 ze dne 21. června 2005 o financování společné zemědělské politiky, Úř. věst. 2005 L 209; a 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.

40 Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR (C-92/09) a Hartmut Eifert (C-93/09) proti Land Hessen*, body 47–52, 58, 66–67, 75, 86 a 92.

zveřejňování informací o příjemcích evropských zemědělských fondů za částečně neplatné.

## 1.2.3. Svoboda umění a věd

Další právo, u něhož je třeba zajistit rovnováhu s právem na respektování soukromého života a na ochranu údajů, je svoboda umění a věd, již výslovně chrání článek 13 Listiny. Toto právo je odvozeno primárně od práva na svobodu myšlení a projevu a musí být vykonáváno s ohledem na článek 1 Listiny (Lidská důstojnost). ESLP se domnívá, že svoboda umění je chráněna podle článku 10 EÚLP.[41] Právo, jež zaručuje článek 13 Listiny, může též podléhat omezením, která povoluje článek 10 EÚLP.[42]

Příklad: Ve věci *Vereinigung bildender Künstler proti Rakousku*[43] rakouské soudy zakázaly sdružení stěžovatele dále vystavovat obraz, který obsahoval fotografie hlav různých významných osob v sexuálních polohách. Poslanec rakouského parlamentu, jehož fotografie byla na obraze použita, zahájil proti sdružení stěžovatele řízení a žádal o vydání předběžného opatření, které by vystavování obrazu zakázalo. Vnitrostátní soud jeho žádosti vyhověl a předběžné opatření vydal. ESLP zopakoval, že článek 10 EÚLP se použije na sdělování myšlenek, které urážejí, šokují nebo znepokojují stát nebo jakoukoli část veřejnosti. Ti, kteří umělecká díla vytvořili, předváděli, distribuovali nebo vystavovali, přispěli k výměně myšlenek a názorů a stát byl povinen nezasahovat nepřiměřeným způsobem do jejich svobody projevu. Vzhledem k tomu, že obraz byl koláž, použité fotografie zobrazovaly pouze hlavy osob a jejich těla byla namalována nerealistickým a přehnaným způsobem, jehož účelem zcela jasně nebylo odrážet skutečnost nebo dokonce tvrdit, že se jedná o skutečnost, ESLP dále uvedl, že *„the painting could hardly be understood to address details of [the depicted's] private life, but rather related to his public standing as a politician"* [obraz lze stěží chápat jako dílo zobrazující detaily soukromého života [vyobrazené osoby], ale vztahuje se spíše k jejímu veřejnému postavení jakožto politikovi] a že *„in this capacity [the depicted] had to display a wider tolerance in respect of criticism"* [z tohoto titulu by [vyobrazená osoba] měla projevit větší toleranci ke kritice]. ESLP zvážil různé zájmy v dané věci a shledal, že neomezený zákaz

41 Rozsudek ESLP ze dne 24. května 1988, *Müller a další proti Švýcarsku*, č. 10737/84.

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

43 Rozsudek ESLP ze dne 25. ledna 2007, *Vereinigung bildender Künstler proti Rakousku*, č. 68345/01, viz zejména body 26 a 34.

dalšího vystavování obrazu byl nepřiměřený. Soud dospěl k závěru, že došlo k porušení článku 10 EÚLP.

Co se týče vědy, evropské právo v oblasti ochrany osobních údajů si je vědomo zvláštní hodnoty, jež věda pro společnost zastává. Proto jsou obecná omezení používání osobních údajů menší. Jak směrnice o ochraně údajů, tak úmluva č. 108 povolují uchovávání údajů pro vědecký výzkum poté, co již nejsou potřeba pro původní účel, pro nějž byly shromážděny. Dále následné používání osobních údajů pro vědecký výzkum se nepovažuje za neslučitelný účel. Úkol vypracovat podrobnější ustanovení, včetně nezbytných ochranných opatření, pro sladění zájmu vědeckého výzkumu s právem na ochranu údajů náleží vnitrostátnímu právu (viz též oddíly 3.3.3 a 8.4).

## 1.2.4. Ochrana vlastnictví

Právo na ochranu vlastnictví je zakotvené v článku 1 prvního protokolu EÚLP a také v čl. 17 odst. 1 Listiny. Jedním z důležitých aspektů práva na vlastnictví je ochrana duševního vlastnictví, kterou výslovně zmiňuje čl. 17 odst. 2 Listiny. V právním řádu EU můžeme najít několik směrnic, jejichž cílem je účinná ochrana duševního vlastnictví, zejména autorského práva. Duševní vlastnictví zahrnuje nejenom literární a umělecké vlastnictví, ale také práva k ochranným známkám, patentová a související práva.

Jak jasně uvádí judikatura Soudního dvora, ochrana základního práva na vlastnictví musí být v rovnováze s ochranou ostatních základních práv, zejména s právem na ochranu údajů.[44] Objevily se případy, kdy instituce zabývající se ochranou autorského práva vyžadovaly, aby poskytovatelé internetových služeb zpřístupnili totožnost uživatelů internetových platforem pro sdílení souborů. Takové platformy často umožňují internetovým uživatelům stahovat hudební tituly zdarma, přestože jsou tyto tituly chráněné autorským právem.

Příklad: Věc *Promusicae proti Telefónica de España*[45] se týkala odmítnutí španělského poskytovatele přístupu k internetu, společnosti Telefónica, zpřístupnit neziskové organizaci hudebních producentů a vydavatelů hudebních a audiovizuálních nahrávek s názvem Promusicae osobní údaje určitých osob, jimž

44 Rozsudek ESLP ze dne 10. ledna 2013, *Ashby Donald a další proti Francii*, č. 36769/08.

45 Rozsudek Soudního dvora ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, body 54 a 60.

poskytovala služby internetového připojení. Promusicae požadovala zpřístupnění informací, aby mohla zahájit občanskoprávní řízení proti osobám, které podle této organizace používaly program na výměnu souborů, jenž poskytoval přístup ke zvukovým záznamům, k nimž drželi užívací práva členové organizace Promusicae.

Španělský soud věc postoupil Soudnímu dvoru a požádal o vyjádření, zda musí být tyto údaje podle práva Společenství sdělovány v souvislosti s občanskoprávním řízením, aby byla zajištěna účinná ochrana autorského práva. Odkazoval na směrnice 2000/31, 2001/29 a 2004/48, vykládané též ve světle článků 17 a 47 Listiny. Soudní dvůr dospěl k závěru, že tyto tři směrnice i směrnice o soukromí a elektronických komunikacích (směrnice 2002/58) nevylučují možnost, aby členské státy stanovily povinnost zpřístupnit osobní údaje v rámci občanskoprávního řízení, aby zajistily účinnou ochranu autorského práva.

Soudní dvůr poukázal na to, že v souvislosti s danou věcí 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.

Soudní dvůr dospěl k závěru, že „členské státy musí 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 provedla ve vnitrostátním právním řádu, orgány a soudy členských států nejen vykládaly své vnitrostátní právo v souladu s uvedenými 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“.[46]

46 *Tamtéž*, body 65 a 68; viz rovněž rozsudek Soudního dvora ze dne 16. února 2012, C-360/10, *SABAM proti Netlog N.V.*

# 2 Terminologie ochrany údajů

| EU | Probíraná témata | RE |
|---|---|---|
| **Osobní údaje** | | |
| Čl. 2 písm. a) směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*<br>Rozsudek Soudního dvora ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU* | **Právní definice** | Čl. 2 písm. a) úmluvy č. 108<br>Rozsudek ESLP ze dne 14. března 2013, *Bernh Larsen Holding AS a další proti Norsku*, č. 24117/08 |
| Čl. 8 odst. 1 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist* | **Zvláštní kategorie osobních údajů (citlivé údaje)** | Článek 6 úmluvy č. 108 |
| Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů | **Anonymizované a pseudonymizované údaje** | Čl. 5 písm. e) úmluvy č. 108<br>Článek 42 důvodové zprávy k úmluvě č. 108 |
| **Zpracování údajů** | | |
| Čl. 2 písm. b) směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist* | **Definice** | Čl. 2 písm. c) úmluvy č. 108 |
| **Uživatelé údajů** | | |
| Čl. 2 písm. d) směrnice o ochraně údajů | **Správce** | Čl. 2 písm. d) úmluvy č. 108<br>Čl. 1 písm. g) doporučení o profilování * |

| EU | Probíraná témata | RE |
|---|---|---|
| Čl. 2 písm. e) směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist* | **Zpracovatel** | Čl. 1 písm. h) doporučení o profilování |
| Čl. 2 písm. g) směrnice o ochraně údajů | **Příjemce** | Čl. 2 odst. 1 dodatkového protokolu k úmluvě č. 108 |
| Čl. 2 písm. f) směrnice o ochraně údajů | **Třetí osoba** | |
| **Souhlas** | | |
| Čl. 2 písm. h) směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG proti Bundesrepublik Deutschland* | **Definice a požadavky platného souhlasu** | Článek 6 doporučení o zdravotnické dokumentaci a různá následná doporučení |

*Poznámka: *Rada Evropy (2010), Výbor ministrů (2010), Doporučení č. Rec(2010)13 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

- Údaje jsou označovány jako osobní údaje, pokud se týkají identifikované nebo alespoň identifikovatelné osoby, subjektu údajů.
- Osoba je identifikovatelná, je-li možné bez nepřiměřeného úsilí získat dodatečné informace, které umožní identifikovat subjekt údajů.
- Ověřením nebo autentizací se rozumí prokázání, že určitá osoba má určitou totožnost a/nebo je oprávněna vykonávat určité činnosti.
- Existují zvláštní kategorie údajů, takzvané citlivé údaje, které jsou uvedeny v úmluvě č. 108 a ve směrnici o ochraně údajů, jež vyžadují zvýšenou ochranu, a podléhají tudíž zvláštnímu právnímu režimu.
- Údaje jsou anonymizovány, pokud již neobsahují žádné identifikátory; jsou pseudonymizovány, pokud jsou identifikátory zašifrovány.
- Na rozdíl od anonymizovaných údajů, pseudonymizované údaje jsou osobními údaji.

## 2.1.1. Hlavní aspekty pojetí osobních údajů

**Podle práva EU** i **podle práva RE** jsou „osobní údaje" definovány jako informace o identifikované nebo identifikovatelné fyzické osobě,[47] to znamená informace o osobě, jejíž totožnost je buď zcela jasná, nebo může být alespoň zjištěna na základě získání dodatečných informací.

Jsou-li údaje o takové osobě zpracovávány, hovoříme o ní jako o „subjektu údajů".

### Osoba

Právo na ochranu údajů se vyvinulo z práva na respektování soukromého života. Pojetí soukromého života se týká lidských bytostí. Fyzické osoby tudíž představují primární příjemce ochrany údajů. V souladu se stanoviskem pracovní skupiny zřízené podle článku 29 je navíc podle evropského práva v oblasti ochrany údajů chráněna pouze *živá bytost*.[48]

Judikatura ESLP týkající se článku 8 EÚLP ukazuje, že může být obtížné zcela oddělit záležitosti soukromého a pracovního života.[49]

Příklad: Ve věci *Amann proti Švýcarsku*[50] orgány odposlechly obchodní telefonní hovor stěžovatele. Na základě uvedeného telefonního hovoru orgány stěžovatele vyšetřovaly a provedly záznam ve vnitrostátním bezpečnostním rejstříku. Přestože se odposlech týkal obchodního telefonního hovoru, podle ESLP se uchovávání údajů o tomto hovoru týkalo soukromého života stěžovatele. Poukázal na to, že pojem „soukromý život" nesmí být vykládán restriktivně, zejména z toho důvodu, že respektování soukromého života zahrnuje právo navazovat a rozvíjet vztahy s ostatními lidskými bytostmi. Navíc zde neexistoval žádný zásadní důvod, který by ospravedlnil vyloučení činností pracovní nebo obchodní povahy z pojmu „soukromého života". Takový široký výklad odpovídal výkladu úmluvy č. 108. ESLP dále shledal, že zásah ve věci stěžovatele nebyl v souladu s právními předpisy, jelikož vnitrostátní právní předpisy neobsahovaly

47 Čl. 2 písm. a) směrnice o ochraně údajů; čl. 2 písm. a) úmluvy č. 108.

48 Pracovní skupina zřízená podle článku 29 (2007), Stanovisko 4/2007 k pojetí osobních údajů, WP 136, 20. června 2007, s. 22.

49 Viz například: Rozsudek ESLP [velkého senátu] ze dne 4. května 2000, *Rotaru proti Rumunsku*, č. 28341/95, bod 43; rozsudek ESLP ze dne 16. prosince 1992, *Niemietz proti Německu*, 13710/88, bod 29.

50 Rozsudek ESLP [velkého senátu] ze dne 16. února 2000, *Amann proti Švýcarsku*, č. 27798/95, bod 65.

zvláštní a podobná ustanovení o shromažďování, záznamu a uchovávání informací. Dospěl tedy k závěru, že došlo k porušení článku 8 EÚLP.

Kromě toho, pokud záležitosti pracovního života mohou být též předmětem ochrany údajů, zdá se diskutabilní, že by ochrana měla být přiznána pouze fyzickým osobám. Práva podle EÚLP jsou zaručena nejenom fyzickým osobám, ale každému.

Judikatura ESLP zahrnuje rozsudky týkající se věcí, v nichž právnické osoby vznesly žalobu proti porušení svého práva na ochranu před tím, aby jejich údaje byly používány, podle článku 8 EÚLP. Soud však tuto věc šetřil podle práva na respektování obydlí a korespondence spíše než soukromého života.

Příklad: Věc *Bernh Larsen Holding AS a další proti Norsku*[51] se týkala stížnosti vznesené třemi norskými společnostmi v souvislosti s rozhodnutím daňového úřadu, jež jim přikazovalo poskytnout daňovým auditorům kopii všech údajů na počítačovém serveru, který tyto tři společnosti společně využívaly.

ESLP shledal, že taková povinnost uložená stěžujícím si společnostem představuje zásah do jejich práva na respektování „obydlí" a „korespondence" pro účel článku 8 EÚLP. Soud však zjistil, že daňové úřady mají účinná a dostatečná ochranná opatření proti zneužití: stěžující si společnosti byly uvědoměny dostatečně dopředu, během zásahu na místě byly přítomné a mohly předložit připomínky a po dokončení daňové kontroly měly být materiály zničeny. Za takových okolností byla zajištěna spravedlivá rovnováha mezi právem stěžujících si společností na respektování „obydlí" a „korespondence" a jejich zájmem na ochranu soukromí osob, jež pro ně pracují, na jedné straně a veřejným zájmem na zaručení účinné kontroly pro účely vyměření daně na straně druhé. Soud proto rozhodl, že nedošlo k porušení článku 8.

**Podle úmluvy č. 108** se ochrana údajů týká primárně ochrany fyzických osob, nicméně smluvní strany mohou ochranu údajů ve vnitrostátních právních předpisech rozšířit na právnické osoby, jako jsou obchodní společnosti a sdružení. **Právo EU v oblasti ochrany údajů** se obecně nevztahuje na ochranu právnických osob, pokud

51 Rozsudek ESLP ze dne 14. března 2013, *Bernh Larsen Holding AS a další proti Norsku*, č. 24117/08. Viz však také rozsudek ESLP ze dne 1. července 2008, *Liberty a další proti Spojenému království*, č. 58243/00.

jde o zpracovávání údajů, jež se jich týkají. Vnitrostátní regulační orgány mají při úpravě této oblasti volnou ruku.[52]

Příklad: Ve věci *Volker und Markus Schecke a Hartmut Eifert proti Land Hessen*[53] Soudní dvůr rozhodl ohledně zveřejňování osobních údajů o příjemcích zemědělské pomoci, že se „právnické osoby 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. […] Respektování 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 […]“.[54]

## Identifikovatelnost osoby

**Podle práva EU** i **podle práva RE** informace obsahují údaje o osobě, jestliže:

- tyto informace osobu identifikují nebo
- osoba, byť neidentifikovaná, je v těchto informacích popsána takovým způsobem, že je možné totožnost subjektu údajů zjistit provedením dalšího šetření.

Oba typy informací jsou v evropském právu v oblasti ochrany údajů chráněny stejným způsobem. ESLP opakovaně uvedl, že pojem „osobní údaje“ podle EÚLP je totožný jako v úmluvě č. 108, zejména co se týče podmínky, že se musí týkat identifikovaných či identifikovatelných osob.[55]

Právní definice osobních údajů blíže neobjasňují, kdy se osoba považuje za identifikovanou.[56] Je zřejmé, že identifikace vyžaduje prvky, které popisují osobu takovým způsobem, že ji lze odlišit od všech ostatních osob a rozpoznat jako jednotlivce. Nejlepším příkladem takového prvku popisu je jméno osoby. Ve výjimečných případech mohou mít podobný účinek jako jméno jiné identifikátory. Například v případě

52 24. bod odůvodnění směrnice o ochraně údajů.

53 Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR (C-92/09) a Hartmut Eifert (C-93/09) proti Land Hessen*, bod 53.

54 *Tamtéž*, bod 52.

55 Viz rozsudek ESLP [velkého senátu] ze dne 16. února 2000, *Amann proti Švýcarsku*, č. 27798/95, bod 65 a další.

56 Viz rovněž rozsudek ESLP [velkého senátu] ze dne 13. února 2003, *Odièvre proti Francii*, č. 42326/98; a rozsudek ESLP ze dne 25. září 2012, *Godelli proti Itálii*, č. 33783/09.

významných osob může stačit uvést pozici dané osoby, například předseda Evropské komise.

> Příklad: Ve věci *Promusicae*[57] Soudní dvůr uvedl, že „není zpochybněno, že sdělení jmen a adres určitých uživatelů [určité internetové platformy pro sdílení souborů], o které žádá sdružení Promusicae, s sebou 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 [...]. Toto sdělení informací, které jsou podle sdružení Promusicae uchovávány společností Telefónica – což posledně uvedená nezpochybňuje – představuje zpracování osobních údajů ve smyslu čl. 2 prvního pododstavce směrnice 2002/58 ve spojení s čl. 2 písm. b) směrnice 95/46."

Jelikož mnoho jmen není jedinečných, může zjištění totožnosti osoby vyžadovat dodatečné identifikátory, aby se zajistilo, že osoba není zaměněna s někým jiným. Často se používá datum a místo narození. Dále byla v některých zemích zavedena osobní čísla, která slouží k lepšímu rozlišování mezi občany. Biometrické údaje, jako jsou otisky prstů, digitální fotografie nebo skeny oční duhovky, nabývají v technologickém věku pro identifikaci osob na významu.

Použitelnost evropského práva v oblasti ochrany údajů však nevyžaduje vysoce kvalitní identifikaci subjektu údajů, stačí, že dotčená osoba je identifikovatelná. Osoba se považuje za identifikovatelnou, pokud informace obsahuje prvky identifikace, na jejichž základě lze osobu přímo či nepřímo identifikovat.[58] V souladu s 26. bodem odůvodnění směrnice o ochraně údajů je měřítkem to, zda je pravděpodobné, že budou k dispozici prostředky, jež mohou být pro identifikaci rozumně použity, a budou spravovány předvídatelnými uživateli informací, což zahrnuje třetí příjemce (viz oddíl 2.3.2).

> Příklad: Místní orgán se rozhodne shromažďovat údaje o vozidlech překračujících rychlost na místních komunikacích. Pořizuje fotografie vozidel, automaticky zaznamenává čas a místo, aby údaje předal příslušnému orgánu a ten mohl řidiče, kteří překročili povolenou rychlost, pokutovat. Subjekt údajů podá stížnost, v níž tvrdí, že místní orgán nemá pro takové shromažďování údajů žádnou

57 Rozsudek Soudního dvora ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU*, bod 45.

58 Čl. 2 písm. a) směrnice o ochraně údajů.

oporu v zákoně o ochraně osobních údajů. Místní orgán se hájí tím, že neshromažďuje osobní údaje. Tvrdí, že registrační značky jsou údaje o anonymních osobách. Místní orgán nemá ze zákona žádné právo na přístup do všeobecného registru vozidel, aby mohl zjistit totožnost vlastníka nebo řidiče vozidla.

Toto odůvodnění není v souladu s 26. bodem odůvodnění směrnice o ochraně údajů. Vzhledem k tomu, že jasným účelem shromažďování údajů je identifikovat a pokutovat řidiče překračující rychlost, lze předpokládat, že bude učiněn pokus o identifikaci. Přestože místní orgány nemají přímo k dispozici prostředky pro identifikaci, předají údaje příslušnému orgánu, policii, který takovými prostředky disponuje. 26. bod odůvodnění výslovně zahrnuje scénář, kdy lze předpokládat, že se o identifikaci osoby mohou pokoušet jiní příjemci údajů než bezprostředný uživatel údajů. Ve světle 26. bodu odůvodnění činnosti místního orgánu odpovídá shromažďování údajů o identifikovatelných osobách, a tudíž vyžaduje právní základ v právu v oblasti ochrany údajů.

**Právo RE** identifikovatelnost chápe shodně. Čl. 1 odst. 2 doporučení týkající se údajů používaných při platebních operacích[59] například uvádí, že se osoba nepokládá za „identifikovatelnou", pokud její identifikace vyžaduje neúměrně dlouhou dobu, náklady nebo lidské zdroje.

## Ověření (autentizace)

Jedná se o postup, na základě kterého je osoba schopna prokázat, že má určitou totožnost a/nebo je oprávněna k výkonu určitých činností, např. ke vstupu do zabezpečené oblasti nebo výběru peněz z bankovního účtu. Ověření lze dosáhnout prostřednictvím porovnání biometrických údajů, jako je fotografie nebo otisky prstů v cestovním pasu, s údaji osoby, jež se představuje, například při imigrační kontrole; nebo vyžádáním si informací, které by měla znát pouze osoba s určitou totožností nebo oprávněním, např. osobní identifikační číslo (tzv. PIN) nebo heslo; nebo požádáním o předložení určitého znaku, který by měla vlastnit pouze osoba s určitou totožností nebo oprávněním, např. speciální čipová karta nebo klíč k bezpečnostní schránce v bance. Kromě hesel nebo čipových karet, někdy společně s číslem PIN, se používají elektronické podpisy, které představují nástroj, jehož pomocí lze identifikovat a ověřit osobu v elektronické komunikaci.

59 RE, Výbor ministrů (1990), Doporučení č. R Rec(90) 19 o ochraně osobních údajů používaných při platebních a jiných souvisejících operacích, 13. září 1990.

## Povaha údajů

Osobními údaji mohou být jakékoli informace, pokud se týkají určité osoby.

Příklad: Hodnocení pracovního výkonu zaměstnance vedoucím archivované v osobní složce zaměstnance představuje osobní údaje o zaměstnanci, přestože může jen odrážet částečně či zcela osobní názor vedoucího, např.: „pracovník není oddaný své práci“ a nikoli jen spolehlivá fakta, např.: „pracovník byl v minulých šesti měsících nepřítomen v práci po dobu šesti týdnů“.

Osobní údaje zahrnují informace týkající se soukromého života osoby i informace o jejím pracovním nebo veřejném životě.

Ve věci *Amann*[60] ESLP vykládal pojem „osobní údaje“ v tom smyslu, že se neomezují na záležitosti soukromé sféry jednotlivce (viz oddíl 2.1.1.). Význam pojmu „osobní údaje“ je též relevantní pro směrnici o ochraně údajů:

Příklad: Ve věci *Volker und Markus Schecke a Hartmut Eifert proti Land Hessen*[61] Soudní dvůr 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“.“

Údaje se týkají osob rovněž tehdy, pokud obsah informací nepřímo odhaluje údaje o osobě. V některých případech, kde existuje úzká souvislost mezi předmětem nebo událostí – např. mobilní telefon, automobil, nehoda – na jedné straně a osobou – např. jeho majitel, uživatel, oběť – na straně druhé, by měly být informace o předmětu nebo o události též považovány za osobní údaje.

Příklad: Ve věci *Uzun proti Německu*[62] stěžovatel a další muž byli sledováni prostřednictvím zařízení globálního systému pro určování polohy (GPS) instalovaného ve vozidle tohoto dalšího muže, jelikož byli podezíráni ze zapojení

60 Viz rozsudek ESLP ze dne 16. února 2000, *Amann proti Švýcarsku*, č. 27798/95, bod 65.

61 Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*, bod 59.

62 Rozsudek ESLP ze dne 2. září 2010, *Uzun proti Německu*, č. 35623/05.

do bombových útoků. V této věci ESLP rozhodl, že sledování stěžovatele přes GPS představuje zásah do jeho soukromého života, který chrání článek 8 EÚLP. Avšak sledování pomocí GPS bylo v souladu se zákonem i přiměřené legitimnímu cíli vyšetřování několika případů pokusů o vraždu, a bylo tudíž v demokratické společnosti nezbytné. Soud rozhodl, že nedošlo k porušení článku 8 EÚLP.

### Forma výskytu údajů

Forma, v níž jsou osobní údaje uchovávány nebo používány, není relevantní pro použitelnost práva v oblasti ochrany údajů. Písemné či ústní komunikace mohou obsahovat osobní údaje i obrazy[63], včetně záznamu z kamerového systému[64] nebo zvukového záznamu.[65] Elektronicky zaznamenané informace i informace v listinné podobě, mohou představovat osobní údaje, i vzorky lidské tkáně mohou být osobními údaji, jelikož nesou informaci o DNA určité osoby.

## 2.1.2. Zvláštní kategorie osobních údajů

**Podle práva EU** i **podle práva RE** existují zvláštní kategorie osobních údajů, které svou povahou mohou při zpracování představovat riziko pro subjekty údajů a vyžadují zvýšenou ochranu. Proto musí být zpracování těchto zvláštních kategorií údajů („citlivé údaje“) povoleno pouze se zvláštními ochrannými opatřeními.

Při definování citlivých údajů jak úmluva č. 108 (článek 6), tak směrnice o ochraně údajů (článek 8) jmenují tyto kategorie:

- osobní údaje, které odhalují rasový či etnický původ,
- osobní údaje, které odhalují politické názory, náboženské nebo jiné přesvědčení,
- osobní údaje týkající se zdraví a sexuálního života.

63 Rozsudek ESLP ze dne 24. června 2004, *Von Hannover proti Německu*, č. 59320/00; rozsudek ESLP ze dne 11. ledna 2005, *Sciacca proti Itálii*, č. 50774/99.

64 Rozsudek ESLP ze dne 28. ledna 2003, *Peck proti Spojenému království*, č. 44647/98; rozsudek ESLP ze dne 5. října 2010, *Köpke proti Německu*, č. 420/07.

65 16. a 17. bod odůvodnění směrnice o ochraně údajů; rozsudek ESLP ze dne 25. září 2001, *P.G. a J.H. proti Spojenému království*, č. 44787/98, body 59 a 60; rozsudek ESLP ze dne 20. prosince 2005, *Wisse proti Francii*, č. 71611/01.

Příklad: Ve věci *Bodil Lindqvist*[66] Soudní dvůr 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 ve smyslu čl. 8 odst. 1 směrnice 95/46".

Směrnice o ochraně osobních údajů jako citlivý údaj uvádí též „odborovou příslušnost", jelikož tyto informace mohou být významným ukazatelem politického přesvědčení nebo příslušnosti.

Úmluva č. 108 za citlivé údaje považuje také osobní údaje týkající se odsouzení za trestný čin.

Čl. 8 odst. 7 směrnice o ochraně údajů členským státům EU ukládá, aby „[určily] podmínky, za kterých může být předmětem zpracování vnitrostátní identifikační číslo nebo jakýkoli jiný identifikátor obecného významu".

## 2.1.3. Anonymizované a pseudonymizované údaje

V souladu se zásadou omezené lhůty pro uchovávání údajů uvedenou ve směrnici o ochraně údajů i v úmluvě č. 108 (kterou se podrobněji zabývá kapitola 3) údaje musejí být uchovávány „ve formě umožňující identifikaci subjektů údajů po dobu ne delší než je nezbytné pro naplnění účelu, pro který jsou shromažďovány nebo dále zpracovávány".[67] Údaje by tudíž musely být anonymizovány, pokud by je správce chtěl uchovávat i poté, co by se staly zastaralými a již by nesloužily původnímu účelu.

### Anonymizované údaje

Údaje jsou anonymizované, byly-li ze souboru osobních údajů odstraněny všechny identifikační prvky. V informacích nesmí být ponechán žádný prvek, který by mohl při vynaložení přiměřeného úsilí sloužit k opětovné identifikaci dotčené osoby či osob.[68] Pokud údaje byly úspěšně anonymizovány, již nejsou osobními údaji.

Jestliže osobní údaje již neslouží svému původnímu účelu, ale mají být ponechány v personalizované podobě pro historické, statistické nebo vědecké použití, směrnice

66 Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*, bod 51.

67 Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů a čl. 5 písm. e) úmluvy č. 108.

68 *Tamtéž*, 26. bod odůvodnění.

o ochraně údajů a úmluva č. 108 tuto možnost povolují pod podmínkou, že jsou přijata vhodná ochranná opatření proti zneužití.[69]

## Pseudonymizované údaje

Osobní údaje obsahují identifikátory, jako je jméno, datum narození, pohlaví a adresa. Když jsou osobní údaje pseudonymizovány, identifikátory se nahradí pseudonymem. Pseudonymizace se dosahuje například pomocí šifrování identifikátorů v osobních údajích.

Pseudonymizované údaje nejsou výslovně uvedeny ani v právních definicích úmluvy č. 108 ani směrnice o ochraně údajů. Avšak článek 42 důvodové zprávy k úmluvě č. 108 uvádí, že *„[t]he requirement [...] concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers"* [požadavek týkající se lhůt pro uchovávání údajů ve formě, kdy jsou spojeny se jménem, neznamená, že by údaje měly být po určité době nenávratně odděleny od jména osoby, k níž se vztahují, ale pouze to, že by nemělo by být možné snadno spojit údaje s identifikátory]. Tohoto výsledku lze dosáhnout pseudonymizací údajů. Pro každého, kdo nedisponuje dešifrovacím klíčem, je velmi obtížné pseudonymizované údaje identifikovat. Odkaz na totožnost stále existuje ve formě pseudonymu a dešifrovacího klíče. Pro ty, kteří jsou oprávněni dešifrovací klíč použít, je opětovná identifikace snadná. Je nezbytné zabezpečit, aby šifrovací klíče nemohly použít neoprávněné osoby.

Jelikož pseudonymizace údajů je jedním z nejdůležitějších prostředků k zajištění ochrany údajů ve velkém rozsahu, pokud není možné osobní údaje přestat zcela používat, je nutné logiku a účinek takového kroku podrobněji vysvětlit.

Příklad: Větu „Charles Spencer, narozen 3. dubna 1967, je otcem čtyř dětí, dvou chlapců a dvou dívek" je například možné pseudonymizovat takto:

„C.S., 1967, je otcem čtyř dětí, dvou chlapců a dvou dívek" nebo

„324 je otcem čtyř dětí, dvou chlapců a dvou dívek" nebo

69 *Tamtéž*, čl. 6 odst. 1 písm. e) a čl. 5 písm. e) úmluvy č. 108.

„YESz320l je otcem čtyř dětí, dvou chlapců a dvou dívek".

Uživatelé, kteří se k těmto pseudonymizovaným údajům dostanou, nebudou schopni identifikovat „Charlese Spencera, narozeného 3. dubna 1967" z „324" nebo „YESz3201". Pseudonymizované údaje jsou tudíž spíše chráněny před zneužitím.

Nicméně první příklad je méně zabezpečený. Je-li věta „C.S., 1967, je otcem čtyř dětí, dvou chlapců a dvou dívek" použita ve vesničce, kde Charles Spencer žije, může být snadné pana Spencera poznat. Způsob pseudonymizace ovlivňuje účinnost ochrany údajů.

Osobní údaje se zašifrovanými identifikátory se používají v řadě situací jako prostředek pro utajení totožnosti osob. To je obzvláště užitečné, když správci údajů potřebují zajistit, že se jedná o stejné subjekty údajů, ale nepotřebují nebo neměli by znát skutečnou totožnost subjektů údajů. Tak tomu například je v situaci, kdy výzkumník zkoumá průběh nemoci u pacientů, jejichž totožnost zná pouze nemocnice, kde jsou léčeni a odkud výzkumník získává pseudonymizované anamnézy. Pseudonymizace tudíž představuje pevné spojení v arzenálu technologie zvyšující ochranu soukromí. Může být důležitým prvkem při provádění ochrany soukromí již od návrhu (tzv. „privacy by design") To znamená, když je ochrana údajů již zakomponovaná do struktury moderních systémů pro zpracovávání údajů.

## 2.2. Zpracování údajů

### Hlavní body

- Pojem „zpracování" se týká převážně automatizovaného zpracování.
- Podle práva EU se „zpracování" týká také manuálního zpracování v uspořádaných rejstřících.
- Podle práva RE je možné význam „zpracování" rozšířit ve vnitrostátním právu tak, aby zahrnovalo manuální zpracování.

Ochrana osobních údajů podle úmluvy č. 108 a směrnice o ochraně údajů se primárně zaměřuje na automatizované zpracování údajů.

Podle **práva RE** definice automatizovaného zpracování však uznává, že mezi automatizovanými operacemi může být zapotřebí několik fází manuálního používání

osobních údajů. Podobně podle **práva EU** se automatizované zpracování údajů definuje jako „operace uskutečňované zcela nebo zčásti pomocí automatizovaných postupů“.[70]

> Příklad: Ve věci *Bodil Lindqvist*[71] Soudní dvůr rozhodl, že:
>
> „[ú]kon, který spočívá v tom, že se na internetové 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“.

Manuální zpracování osobních údajů také vyžaduje jejich ochranu.

Ochrana údajů **podle práva EU** se v žádném případě neomezuje na automatizované zpracování údajů. Podle práva EU se ochrana údajů tudíž vztahuje na zpracování osobních údajů v manuálních rejstřících, tedy ve speciálně uspořádaných listinných složkách.[72] Důvodem tohoto rozšíření ochrany údajů je, že:

- listinné složky lze uspořádat tak, aby se v nich informace vyhledávaly rychle a snadno, a
- při uchovávání osobních údajů v uspořádaných listinných složkách lze snadno obejít omezení stanovená právními předpisy pro automatizované zpracování údajů.[73]

**Podle práva RE**, zpracování údajů v automatizovaných souborech dat upravuje zejména úmluva č. 108.[74] Také však stanoví možnost rozšíření ochrany na manuální zpracování ve vnitrostátním právu. Mnoho stran úmluvy č. 108 této možnosti využilo a zaslalo v tomto smyslu prohlášení generálnímu tajemníkovi RE.[75] Rozšíření ochrany údajů v souladu s takovým prohlášením se musí týkat veškerého

70 Čl. 2 písm. c) úmluvy č. 108 a čl. 2 písm. b) a čl. 3 odst. 1 směrnice o ochraně údajů.

71 Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*, bod 27.

72 Čl. 3 odst. 1 směrnice o ochraně údajů.

73 *Tamtéž*, 27. bod odůvodnění.

74 Čl. 2 písm. b) úmluvy č. 108.

75 Viz prohlášení učiněná podle čl. 3 odst. 2 písm. c) úmluvy č. 108.

manuálního zpracování údajů a nemůže být omezeno na zpracování v manuálních rejstřících.[76]

Co se týče povahy zahrnutých zpracování, pojem zpracování je komplexní **podle práva EU i podle práva RE**: „‚zpracováním osobních údajů' […] [se rozumí] jakýkoli úkon […], jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace"[77] osobních údajů. Pojem „zpracování" zahrnuje také činnosti, kdy za údaje přestává odpovídat jeden správce a jsou předány jinému správci, který za ně přebírá odpovědnost.

Příklad: Zaměstnavatelé shromažďují a zpracovávají údaje o svých zaměstnancích, včetně informací týkajících se jejich platů. Právním základem k tomu, aby tak mohli legitimně činit, je pracovní smlouva.

Zaměstnavatelé musí předávat údaje o platech svých zaměstnanců daňovým úřadům. Toto předávání údajů také představuje „zpracování" ve smyslu tohoto pojmu v úmluvě č. 108 a ve směrnici. Avšak právním základem takového sdělení není pracovní smlouva. Pro zpracování, jehož výsledkem je předání údajů o platu zaměstnavatelem daňovému úřadu, musí existovat další, speciální právní předpis. Tento právní základ zpravidla obsahují ustanovení vnitrostátních daňových právních předpisů. Bez takových ustanovení by předávaní údajů představovalo nezákonné zpracování.

## 2.3. Uživatelé osobních údajů

### Hlavní body

- Každý, kdo se rozhodne zpracovávat osobní údaje druhých, se podle práva v oblasti ochrany údajů nazývá „správcem". Pokud se takto rozhodne několik osob dohromady, mohou být nazýváni „společnými správci".
- „Zpracovatel" je právně oddělený subjekt, který zpracovává osobní údaje pro správce.

76 Viz znění čl. 3 odst. 2 úmluvy č. 108.

77 Čl. 2 písm. b) směrnice o ochraně údajů. Podobně rovněž viz čl. 2 písm. c) úmluvy č. 108.

- Zpracovatel se stává správcem, pokud používá údaje pro své vlastní účely a nikoli podle pokynů správce.
- Každý, kdo obdrží údaje od správce, se nazývá „příjemcem".
- „Třetí osoba" je fyzická nebo právnická osoba, která nejedná podle pokynů správce (a není subjektem údajů).
- „Třetí příjemce" je osoba nebo subjekt, který je právně oddělený od správce, ale přijímá od něj osobní údaje.

## 2.3.1. Správci a zpracovatelé

Nejvýznamnějším důsledkem zastávání úlohy správce nebo zpracovatele je právní odpovědnost za dodržování příslušných povinností podle práva v oblasti ochrany údajů. Tyto funkce tudíž mohou zastávat pouze subjekty, které mohou podle platného práva nést odpovědnost. V soukromém sektoru to zpravidla bývá fyzická nebo právnická osoba; ve veřejném sektoru to zpravidla bývá úřad se svěřenou pravomocí. Další subjekty, jako jsou orgány nebo instituce bez právní subjektivity, mohou být správci či zpracovateli pouze, pokud to stanoví zvláštní zákonná ustanovení.

Příklad: Pokud marketingové oddělení společnosti Sunshine hodlá zpracovávat údaje pro marketingový průzkum, bude při takovém zpracování správcem společnost Sunshine a nikoli marketingové oddělení. Marketingové oddělení nemůže být správcem, jelikož nemá samostatnou právní subjektivitu.

Ve skupině společností se mateřská společnost a každá přidružená společnost považují za samostatné správce nebo zpracovatele, jelikož se jedná o oddělené právnické osoby. V důsledku tohoto právně odděleného stavu bude předávání údajů mezi členy skupiny společností vyžadovat zvláštní právní základ. Neexistuje žádné oprávnění, jež by povolovalo výměnu osobních údajů jako takovou mezi oddělenými právnickými subjekty v rámci skupiny společností.

V této souvislosti je třeba zmínit úlohu soukromých osob. **Podle práva EU** soukromé osoby, které zpracovávají údaje o druhých v rámci výlučně osobní nebo domácí činnosti, nespadají do působnosti směrnice o ochraně údajů a nepovažují se za správce.[78]

78 12. bod odůvodnění a poslední odrážka čl. 3 odst. 2 směrnice o ochraně údajů.

Avšak judikatura shledala, že uvedený právní předpis o ochraně údajů se nicméně použije, pokud soukromá osoba zveřejňuje údaje o druhých při používání internetu.

Příklad: Ve věci *Bodil Lindqvist*[79] Soudní dvůr trval na tom, že:

„úkon, kdy se na internetové stránce odkáže na různé osoby a tyto jsou identifikovány buď svým jménem, nebo jinými prostředky [...] je „zcela nebo částečně automatizovaným zpracováním osobních údajů" ve smyslu čl. 3 odst. 1 směrnice 95/46."[80]

Takové zpracovávání osobních údajů nespadá do výlučně osobních nebo domácích činností, které nespadají do působnosti směrnice o ochraně osobních údajů, jelikož 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".[81]

## Správce

**Podle práva EU** je správce definován jako subjekt, který „sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů".[82] Rozhodnutí správce stanoví účel a způsob zpracování údajů. **Podle práva RE** definice „správce" navíc zmiňuje, že správce rozhoduje o tom, které kategorie osobních údajů by měly být uloženy.[83]

Úmluva č. 108 ve své definici správce odkazuje na další aspekt správy, který je třeba vzít v potaz. Tato definice zmiňuje otázku, kdo může v souladu se zákonem zpracovávat určité údaje pro určitý účel. Avšak kde dochází k údajně nezákonnému zpracovávání a je nutné najít odpovědného správce, bude za správce považována osoba nebo subjekt, jako je společnost nebo orgán, který rozhodl o tom, že se údaje mají

79 Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*.

80 *Tamtéž*, bod 27.

81 *Tamtéž*, bod 47.

82 Čl. 2 písm. d) směrnice o ochraně údajů.

83 Čl. 2 písm. d) úmluvy č. 108.

zpracovat, bez ohledu na to, zda k tomu byl ze zákona oprávněn či nikoli[84]. Žádost o výmaz musí být tudíž vždy adresována „faktickému" správci.

## Společná správa

Definice „správce" ve směrnici o ochraně údajů stanoví, že se též může jednat o několik právně oddělených subjektů, které dohromady nebo společně s jinými jednají jako správce. To znamená, že společně rozhodují o zpracovávání údajů pro účel, jejž sdílejí.[85] To je ze zákona možné, ovšem pouze v případech, kde existuje zvláštní právní základ, který stanoví společné zpracovávání údajů pro společný účel.

Příklad: Databáze neplatících klientů, kterou společně provozuje několik úvěrových institucí, je běžným příkladem společné správy. Pokud někdo požádá o úvěr u banky, která je jedním ze společných správců, banka zkontroluje databázi, na základě čehož může učinit informované rozhodnutí o úvěruschopnosti žadatele.

Nařízení výslovně neuvádějí, zda společná správa vyžaduje, aby správci sdíleli stejný účel, nebo zda postačí, pokud se jejich účely pouze částečně překrývají. Na úrovni Evropské unie však ještě není k dispozici žádná příslušná judikatura a nejsou též zcela jasné důsledky týkající se odpovědnosti. Pracovní skupina zřízená podle článku 29 je zastáncem širšího výkladu pojmu společné správy, což umožní určitou flexibilitu s cílem pokrýt rostoucí složitost stávající reality v oblasti zpracování údajů.[86] Stanovisko pracovní skupiny dokládá věc týkající se Společnosti pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication, SWIFT).

Příklad: V takzvané věci SWIFT evropské bankovní instituce společnost SWIFT najaly, nejprve jako zpracovatele, aby zajišťovala předávání údajů při bankovních transakcích. SWIFT tyto údaje o bankovních transakcích uložené v operačním středisku ve Spojených státech zpřístupnila Ministerstvu financí USA, aniž by k tomu dostala výslovný příkaz od evropských bankovních institucí, které ji najaly. Při posuzování zákonné povahy této situace pracovní skupina zřízená

84 Viz též pracovní skupina zřízená podle článku 29 (2010), Stanovisko 1/2010 k pojmům „správce" a „zpracovatel", WP 169, Brusel, 16. února 2010, s. 15.

85 Čl. 2 písm. d) směrnice o ochraně údajů.

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

podle článku 29 dospěla k závěru, že evropské bankovní instituce, které služby společnosti SWIFT využívají, jakož i sama společnost SWIFT, musejí být považovány za společné správce odpovědné vůči evropským klientům za zpřístupnění jejich údajů orgánům Spojených států.[87] Společnost SWIFT svým rozhodnutím ohledně zpřístupnění nezákonným způsobem převzala úlohu správce a bankovní instituce evidentně nesplnily svoji povinnost dohledu nad svým zpracovatelem, a proto nemohou být zcela zproštěny odpovědnosti jako správci. Výsledkem této situace je společná správa.

## Zpracovatel

Zpracovatel je v **právu EU** definován jako subjekt, který zpracovává osobní údaje pro správce.[88] Činnosti, jimiž je zpracovatel pověřen, mohou být omezeny na velmi specifický úkol nebo situaci nebo mohou být poměrně obecné a komplexní.

**V právu RE** je význam zpracovatele totožný s právem EU.

Kromě zpracovávání údajů pro druhé budou zpracovatelé též sami správci údajů ve vztahu ke zpracování, které provádějí pro vlastní účely, tedy pro správu vlastních zaměstnanců, prodeje a účtů.

Příklady: Společnost Everready se specializuje na zpracování údajů v oblasti správy údajů lidských zdrojů pro jiné společnosti. V rámci této funkce je společnost Everready zpracovatelem.

Ovšem když Everready zpracovává údaje o svých vlastních zaměstnancích, je správcem zpracování údajů pro účely plnění svých povinností jako zaměstnavatele.

## Vztah mezi správcem a zpracovatelem

Jak jsme již viděli, správce je definován jako subjekt, který určuje účely a prostředky zpracování.

87 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.

88 Čl. 2 písm. e) směrnice o ochraně údajů.

Příklad: Ředitel společnosti Sunshine se rozhodne, že společnost Moonlight, specialista na analýzu trhu, by měla provést analýzu trhu údajů o zákaznících společnosti Sunshine. Přestože úkol určit prostředky zpracování bude takto delegován na společnost Moonlight, společnost Sunshine zůstává správcem a Moonlight je pouze zpracovatelem, jelikož podle smlouvy může Moonlight používat údaje společnosti Sunshine o zákaznících pouze pro účely, jež stanoví společnost Sunshine.

Jestliže je pravomoc určit prostředky zpracování delegována na zpracovatele, správce musí přesto mít možnost zasahovat do rozhodnutí zpracovatele o prostředcích zpracování. Celková odpovědnost stále spočívá na správci, který musí na zpracovatele dohlížet, aby zajistil, že jejich rozhodnutí jsou v souladu s právem v oblasti ochrany údajů. Smlouva, která správci zakazuje zasahovat do rozhodnutí zpracovatele, by tak pravděpodobně byla vykládána ve smyslu společné správy, kdy obě strany sdílejí právní odpovědnost správce.

Pokud by navíc zpracovatel nedodržoval omezení užívání údajů stanovené správcem, zpracovatel by se stal správcem minimálně v rozsahu, v jakém porušil pokyny správce. Tím se zpracovatel s největší pravděpodobností stane správcem, který jedná nezákonně. Původní správce naopak bude muset vysvětlit, jak je možné, aby zpracovatel jednal v rozporu se svým oprávněním. Ovšem pracovní skupina zřízená podle článku 29 se kloní k tomu, aby v takových případech byla předpokládána společné správa, jelikož jsou tak lépe chráněny zájmy subjektů údajů.[89] Podstatným důsledkem společné správy by měla být společná a nerozdílná odpovědnost za škody, která subjektům údajů poskytuje širší spektrum opravných prostředků.

Mohou se rovněž vyskytnout problémy týkající se rozdělení odpovědnosti, kdy správcem je malý podnik a zpracovatelem velká společnost, která si může diktovat podmínky týkající se služeb, jež poskytuje. V takových situacích však pracovní skupina zřízená podle článku 29 tvrdí, že by nemělo dojít ke snížení standardu odpovědnosti na základě ekonomické nerovnováhy a že výklad pojmu správce musí být zachován.[90]

89 Pracovní skupina zřízená podle článku 29 (2010), Stanovisko 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.

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

Z důvodu srozumitelnosti a průhlednosti by detaily vztahu mezi správcem a zpracovatelem měly být zaznamenány v písemné smlouvě.[91] Neexistence takové smlouvy představuje porušení povinnosti správce předložit písemnou dokumentaci o vzájemných povinnostech a mohla by vést k uvalení sankcí.[92]

Zpracovatelé by mohli chtít delegovat některé úkoly na další dílčí zpracovatele. To je právně přípustné a závisí na smluvních ujednáních mezi správcem a zpracovatelem, včetně toho, zda je v každém jednotlivém případě nutné povolení správce nebo zda postačí pouhé jeho nformování.

**Podle práva RE** se výklad pojmů správce a zpracovatele, jak je vysvětleno výše, plně použije, jak ukazují doporučení, která byla vypracována v souladu s úmluvou č. 108.[93]

## 2.3.2. Příjemci a třetí osoby

Rozdíl mezi těmito dvěma kategoriemi osob nebo subjektů, které byly zavedeny ve směrnici o ochraně údajů, spočívá převážně v jejich vztahu ke správci, a tím pádem v jejich povolení přístupu k osobním údajům spravovaným správcem.

„Třetí osoba" je subjekt, který se po právní stránce liší od správce. Zpřístupnění údajů třetí osobě tudíž vždy bude vyžadovat zvláštní právní základ. V souladu s čl. 2 písm. f) směrnice o ochraně údajů se třetí osobou rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt jiný než subjekt údajů, než správce, než zpracovatel a než osoby přímo podléhající správci nebo zpracovateli, které jsou oprávněny ke zpracování údajů". To znamená, že osoby pracující pro organizaci, která je po právní stránce odlišná od správce, i když patří do stejné skupiny nebo holdingu společností, budou obvykle „třetími osobami" (nebo do nich patřit). Na druhou stranu pobočky banky spravující účty klientů z přímého pověření svého ústředí nebudou „třetími osobami".[94]

„Příjemce" je širší pojem než „třetí osoba". Ve smyslu čl. 2 písm. g) směrnice o ochraně údajů se příjemcem rozumí „fyzická nebo právnická osoba, orgán veřejné

91 Čl. 17 odst. 3 a 4 směrnice o ochraně údajů.

92 Pracovní skupina zřízená podle článku 29 (2010), Stanovisko 1/2010 k pojmům „správce" a „zpracovatel", WP 169, Brusel, 16. února 2010, s. 27.

93 Viz např. článek 1 doporučení o profilování.

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

moci, agentura nebo jakýkoli jiný subjekt, kterým jsou údaje sdělovány, ať se jedná či nikoli o třetí osobu". Tímto příjemcem může být osoba mimo správce nebo zpracovatele – to bude tedy třetí osoba – nebo někdo v rámci správce nebo zpracovatele, například zaměstnanec nebo jiné oddělení ve stejné společnosti nebo orgánu.

Rozlišení mezi příjemci a třetími osobami je důležité pouze kvůli podmínkám zákonného zpřístupňování údajů. Zaměstnanci správce nebo zpracovatele mohou být bez dalšího zákonného požadavku příjemci osobních údajů, pokud se podílejí na zpracovávání prováděném správcem nebo zpracovatelem. Na druhou stranu, třetí osoba, která je právně oddělená od správce nebo zpracovatele, není oprávněna používat osobní údaje zpracovávané správcem, s výjimkou zvláštních zákonných důvodů v určitém konkrétním případě. „Třetí příjemci" údajů budou tedy vždy vyžadovat právní základ k tomu, aby mohli zákonným způsobem přijímat osobní údaje.

Příklad: Zaměstnanec zpracovatele, který používá osobní údaje v rámci úkolů zadaných zaměstnavatelem, je příjemcem údajů, ale ne třetí osobou, jelikož údaje používá jménem nebo na základě pokynů zpracovatele.

Pokud se však tentýž zaměstnanec rozhodne použít údaje, k nimž má přístup jako zaměstnanec zpracovatele, pro vlastní účely a prodá je jiné společnosti, pak takový zaměstnanec jedná jako třetí osoba. Již se neřídí příkazy zpracovatele (zaměstnavatele). Jako třetí osoba by zaměstnanec musel mít právní základ pro získání a prodej údajů. V tomto příkladu zaměstnanec takový právní základ zcela jistě nemá, a proto je takové jednání nezákonné.

## 2.4. Souhlas

### Hlavní body

- Souhlas jako právní základ pro zpracování osobních údajů musí být svobodný, vědomý a výslovný.
- Souhlas musí být poskytnut jednoznačně. Souhlas může být poskytnut buď výslovně, nebo implicitně, kdy subjekt údajů jedná tak, že není pochyb o tom, že se zpracováním svých údajů souhlasí.
- Zpracování citlivých údajů na základě souhlasu vyžaduje výslovný souhlas.
- Souhlas lze kdykoli odvolat.

Souhlasem se rozumí „jakýkoli svobodný, výslovný a vědomý projev vůle“.[95] V řadě případů tvoří právní základ pro zákonné zpracování údajů (viz oddíl 4.1).

## 2.4.1. Prvky platného souhlasu

**Právo EU** stanoví tři prvky, které souhlas musí mít, aby byl platný, jejichž cílem je zaručit, že subjekty údajů skutečně chtěly s používáním svých údajů souhlasit:

- na subjekt údajů nesmí být vyvíjen při udělování souhlasu žádný nátlak,
- subjekt údajů musí být řádně informován o předmětu a důsledcích poskytnutí souhlasu,
- rozsah souhlasu musí být přiměřeně konkrétní.

Pouze pokud jsou splněny všechny tyto požadavky, je souhlas platný ve smyslu práva v oblasti ochrany údajů.

Úmluva č. 108 neobsahuje definici souhlasu; to je ponecháno vnitrostátnímu právu. Avšak **podle práva RE** prvky platného souhlasu odpovídají prvkům vysvětleným výše, jak stanoví doporučení vypracovaná v souladu s úmluvou č. 108.[96] Požadavky na souhlas jsou stejné jako na platné prohlášení o záměru podle evropského občanského práva.

Další požadavky na platný souhlas podle občanského práva, jako je způsobilost k právům a právním úkonům, přirozeně platí také v kontextu ochrany údajů, jelikož představují základní právní předpoklady. Neplatný souhlas osob, které nejsou způsobilé k právním úkonům, bude mít za následek neexistenci právního základu pro zpracování údajů o takových osobách.

Souhlas lze poskytnout výslovně,[97] nebo nevýslovně. V prvním případě není pochyb o záměrech subjektu údajů a takový souhlas může být poskytnut buď ústně, nebo písemně. Nevýslovný souhlas se odvozuje ze situace. Každý souhlas musí být poskytnut jednoznačně.[98] To znamená, že by neměla existovat žádná přiměřená

95 Čl. 2 písm. h) směrnice o ochraně údajů.

96 Viz např. úmluva č. 108, bod 6 doporučení o statistických údajích.

97 Čl. 8 odst. 2 směrnice o ochraně údajů.

98 *Tamtéž*, čl. 7 písm. a) a čl. 26 odst. 1.

pochybnost ohledně toho, že subjekt údajů chtěl dát své svolení ke zpracovávání jeho údajů. Například pokud je souhlas odvozen z pouhé nečinnosti, nemůže být považován za jednoznačný. Pokud jsou údaje, které mají být zpracovány, citlivé, je výslovný souhlas povinný a musí být jednoznačný.

## Svobodný souhlas

Existence svobodného souhlasu platí pouze tehdy, *„if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent"* [pokud je subjekt údajů schopen učinit skutečnou volbu a nehrozí nebezpečí podvodu, zastrašování, nátlaku nebo významné negativní důsledky v případě neposkytnutí souhlasu].[99]

Příklad: Na mnoha letištích musí cestující procházet tzv. tělesnými skenery, aby se dostali do prostoru pro nástup do letadla.[100] Vzhledem k tomu, že se při skenování zpracovávají údaje cestujících, musí toto zpracování splňovat jeden z právních důvodů podle článku 7 směrnice o ochrany údajů (viz oddíl 4.1.1). Průchod tělesnými skenery je někdy cestujícím prezentován jako možnost, čímž se naznačuje, že jejich souhlas by mohl odůvodnit zpracování. Cestující by se však mohli obávat, že pokud by odmítli tělesným skenerem projít, vzbudili by podezření nebo se vystavili další kontrole, jako je tělesná prohlídka. Mnoho cestujících se skenováním souhlasí, protože se tak vyvarují případných problémů nebo zdržení. Takový souhlas pravděpodobně není dostatečně svobodný.

Řádný právní základ lze tudíž nalézt v aktu zákonodárce, na základě čl. 7 písm. e) směrnice o ochraně údajů, který stanoví povinnost cestujících spolupracovat v důsledku převažujícího veřejného zájmu. Takové právní předpisy by přesto mohly stanovit možnost volby mezi skenováním a prohledáním, ale pouze v rámci dodatečných opatření hraniční kontroly nezbytných za určitých okolností. Právě toto Evropská komise stanovila ve dvou nařízeních o bezpečnostních skenerech v roce 2011.[101]

99 Viz rovněž pracovní skupina zřízená podle článku 29 (2011), Stanovisko 15/2011 k pojmu „souhlas", WP 187, Brusel, 13. července 2011, s. 12.

100 Tento příklad je převzat z téhož dokumentu, s. 15.

101 Nařízení Komise (EU) č. 1141/2011 ze dne 10. listopadu 2011, kterým se mění nařízení Komise (ES) č. 272/2009, kterým se doplňují společné základní normy ochrany civilního letectví před protiprávními činy, pokud jde o používání bezpečnostních skenerů na letištích EU, Úř. věst. 2011 L 293, a prováděcí nařízení Komise (EU) č. 1147/2011 ze dne 11. listopadu 2011, kterým se mění nařízení Komise (EU) č. 185/2010, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti, pokud jde o používání bezpečnostních skenerů na letištích EU, Úř. věst. 2011 L 294.

Svobodný souhlas by mohl být ohrožen též v situacích podřízenosti, kde existuje významná ekonomická či jiná nerovnováha mezi správcem zajišťujícím souhlas a subjektem údajů, který souhlas poskytuje.[102]

Příklad: Velká společnost hodlá sestavit adresář obsahující jména všech zaměstnanců, jejich funkci ve společnosti a jejich pracovní adresy pouze za účelem zlepšení interní komunikace ve společnosti. Vedoucí personálního oddělení navrhne, aby se ke každému zaměstnanci v adresáři přidala fotografie, aby bylo například snazší poznat kolegy na schůzích. Zástupci zaměstnanců vyžadují, aby to bylo provedeno pouze se souhlasem jednotlivých zaměstnanců.

V takové situaci by souhlas zaměstnance měl být považován za právní základ pro zpracování fotografie v adresáři, jelikož je jasné, že zveřejnění fotografie v adresáři nemá samo o sobě negativní důsledky a navíc je přesvědčivé, že zaměstnanec nebude čelit negativním dopadům ze strany zaměstnavatele, pokud s uveřejněním své fotografie v adresáři nebude souhlasit.

To však neznamená, že souhlas nemůže být nikdy platný v situaci, kdy by jeho neposkytnutí mělo negativní důsledky. Pokud například v důsledku neposkytnutí souhlasu se zákaznickou kartou v supermarketu zákazník neobdrží slevy z cen určitého zboží, souhlas přesto představuje platný právní základ pro zpracování osobních údajů těch zákazníků, kteří s takovou kartou souhlasili. Neexistuje situace podřízenosti mezi společností a zákazníkem a důsledky neposkytnutí souhlasu nejsou dostatečně závažné, aby subjektu údajů neumožňovaly svobodnou volbu.

Na druhou stranu, pokud lze dostatečně významné zboží nebo služby získat pouze a výlučně, jestliže jsou třetím osobám zpřístupněny určité osobní údaje, souhlas subjektu údajů se zpřístupněním jeho údajů zpravidla nelze považovat za svobodné rozhodnutí, a tudíž podle práva v oblasti ochrany údajů není platný.

Příklad: Svolení, které vyjadřují cestující letecké společnosti, s tím, aby předala tzv. jmennou evidenci cestujících (PNR) imigračním orgánům určité cizí země, jmenovitě údaje o jejich totožnosti, stravovacích návycích nebo zdravotních problémech, nelze považovat za platný souhlas podle práva v oblasti ochrany

102 Viz rovněž pracovní skupina zřízená podle článku 29 (2001), Stanovisko 8/2001 ke zpracování osobních údajů v pracovněprávním kontextu, 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.

údajů, jelikož cestující nemají na výběr, pokud chtějí tuto zemi navštívit. Aby takové údaje mohly být předávány zákonným způsobem, je zapotřebí jiný právní základ než souhlas: zpravidla zvláštní právní předpis.

## Vědomý souhlas

Subjekt údajů musí mít předtím, než se rozhodne, dostatečné informace. O tom, zda informace jsou či nejsou dostatečné, je možné rozhodovat pouze případ od případu. Součástí vědomého souhlasu obvykle bývá přesný a snadno srozumitelný popis věci vyžadující souhlas a dále výčet důsledků poskytnutí či neposkytnutí souhlasu. Způsob formulování informací by měl být přizpůsoben předpokládaným příjemcům informací.

Informace musí být subjektu údajů snadno dostupné. Dostupnost a viditelnost informací jsou důležitými prvky. V internetovém prostředí může být vhodné použít vrstvená informační oznámení, takže subjekt údajů má k dispozici stručnou i obsáhlejší verzi informací.

## Výslovný souhlas

Aby souhlas byl platný, musí být také výslovný. To jde ruku v ruce s kvalitou informací poskytnutých ohledně předmětu souhlasu. V této souvislosti budou relevantní přiměřená očekávání průměrného subjektu údajů. Subjekt údajů musí být o poskytnutí souhlasu požádán znovu, pokud mají být přidány nebo změněny nějaké úkony v rámci zpracování způsobem, který nebylo možné přiměřeně předpokládat v okamžiku poskytnutí původního souhlasu.

Příklad: Ve věci *Deutsche Telekom AG*[103] se Soudní dvůr zabýval otázkou, zda poskytovatel telekomunikačních služeb, který měl předat osobní údaje o účastnících podle článku 12 *směrnice o soukromí a elektronických komunikacích*,[104] potřeboval od subjektů údajů obnovený souhlas, jelikož příjemci nebyli při poskytnutí původního souhlasu uvedeni.

103 Rozsudek Soudního dvora ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG proti Německu,* viz zejména body 53 a 54.

104 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*).

Soudní dvůr rozhodl, že podle uvedeného článku není obnovený souhlas před předáním údajů nutný, protože subjekty údajů měly podle tohoto ustanovení možnost poskytnout souhlas pouze s účelem zpracování, což je zveřejnění jejich údajů, a nemohly si vybrat mezi různými účastnickými seznamy, v nichž by tyto údaje mohly být zveřejněny.

Jak Soudní dvůr 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."[105] Navíc „samotné zveřejnění osobních údajů v účastnickém seznamu majícím zvláštní účel může účastníka poškodit"[106] a nikoli autor zveřejnění.

## 2.4.2. Právo souhlas kdykoli odvolat

Směrnice o ochraně údajů nezmiňuje obecné právo kdykoli souhlas odvolat. Nicméně obecně se předpokládá, že takové právo existuje a že subjekt údajů musí mít možnost je dle svého uvážení uplatnit. Při odvolání souhlasu by nemělo být požadováno uvedení důvodů a rovněž by neměly hrozit jiné negativní důsledky kromě ukončení jakýchkoli výhod, které mohly být poskytovány na základě předchozího svolení k užívání údajů.

Příklad: Zákazník souhlasí s přijímáním reklamních materiálů na adresu, kterou poskytne správci údajů. Pokud se zákazník rozhodne souhlas odvolat, správce musí okamžitě zasílání reklamních materiálů ukončit. To by nemělo mít žádné represivní důsledky, např. poplatky.

Jestliže zákazník získal 5% slevu z ceny hotelového pokoje na základě svolení s tím, aby jeho údaje byly používány pro zasílání reklamních materiálů, neměla by skutečnost, kdy zákazník později svůj souhlas s přijímáním reklamních materiálů odvolá, mít za následek povinnost tuto slevu vrátit.

105 Rozsudek Soudního dvora ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG proti Německu,* viz zejména bod 61.

106 *Tamtéž*, viz zejména bod 62.

# 3

# Základní zásady evropského práva v oblasti ochrany údajů

| EU | Probíraná témata | RE |
|---|---|---|
| Čl. 6 odst. 1 písm. a) a b) směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu*<br>Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR (C-92/09) a Hartmut Eifert (C-93/09) proti Land Hessen* | **Zásada zákonného zpracování** | Čl. 5 písm. a) a b) úmluvy č. 108<br>Rozsudek ESLP [velkého senátu] ze dne 4. května 2000, *Rotaru proti Rumunsku*, č. 28341/95<br>Rozsudek ESLP ze dne 22. října 2002, *Taylor-Sabori proti Spojenému království*, č. 47114/99<br>Rozsudek ESLP ze dne 28. ledna 2003, *Peck proti Spojenému království*, č. 44647/98<br>Rozsudek ESLP ze dne 18. října 2011, *Khelili proti Švýcarsku*, č. 16188/07<br>Rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81 |
| Čl. 6 odst. 1 písm. b) směrnice o ochraně údajů | **Zásada specifikace a omezení účelu** | Čl. 5 písm. b) úmluvy č. 108 |
| | **Zásady kvality údajů:** | |
| Čl. 6 odst. 1 písm. c) směrnice o ochraně údajů | **Relevantnost údajů** | Čl. 5 písm. c) úmluvy č. 108 |

| EU | Probíraná témata | RE |
|---|---|---|
| Čl. 6 odst. 1 písm. d) směrnice o ochraně údajů | Přesnost údajů | Čl. 5 písm. d) úmluvy č. 108 |
| Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů | Omezená lhůta pro uchovávání údajů | Čl. 5 písm. e) úmluvy č. 108 |
| Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů | Výjimky pro vědecký výzkum a statistiky | Čl. 9 odst. 3 úmluvy č. 108 |
| Čl. 6 odst. 1 písm. a) směrnice o ochraně údajů | Zásada korektního zpracovávání | Čl. 5 písm. a) úmluvy č. 108<br>Rozsudek ESLP ze dne 27. října 2009, *Haralambie proti Rumunsku*, č. 21737/03<br>Rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další proti Slovensku*, č. 32881/04 |
| Čl. 6 odst. 2 směrnice o ochraně údajů | Zásada odpovědnosti | |

V zásadách stanovených v článku 5 úmluvy č. 108 je zakotvena podstata evropského práva v oblasti ochrany údajů. Jsou uvedeny také v článku 6 směrnice o ochraně údajů jako výchozí bod pro podrobnější ustanovení v následujících článcích směrnice. Všechny pozdější právní předpisy o ochraně údajů na úrovni RE nebo EU musejí být v souladu s těmito zásadami a na tyto zásady je nutno pamatovat při výkladu takových předpisů. Jakékoli výjimky z těchto základních zásad nebo jejich omezení mohou být stanoveny na vnitrostátní úrovni;[107] musí být stanoveny zákonem, sledovat legitimní cíl a být nezbytné v demokratické společnosti. Splněny musí být všechny tři podmínky.

## 3.1. Zásada zákonného zpracování

### Hlavní body

- Pro pochopení zásady zákonného zpracování je třeba poukázat na podmínky zákonného omezení práva na ochranu údajů ve světle čl. 52 odst. 1 Listiny a požadavky oprávněného zásahu podle čl. 8 odst. 2 EÚLP.

107 Čl. 9 odst. 2 úmluvy č. 108; článek 13 směrnice o ochraně údajů.

- Zpracování osobních údajů je podle toho prováděné zákonným způsobem pouze tehdy, když:
  - je v souladu se zákonem a
  - sleduje legitimní účel a
  - je nezbytné v demokratické společnosti v zájmu dosažení legitimního účelu.

**Podle práva EU a RE v oblasti ochrany údajů** je zásada zákonného zpracování první uvedenou zásadou; je vyjádřena téměř shodně v článku 5 úmluvy č. 108 a v článku 6 směrnice o ochraně údajů.

V žádném z těchto ustanovení však není definováno, co se rozumí „zákonným zpracováním". K pochopení tohoto výrazu je třeba odkázat na oprávněný zásah podle EÚLP vykládaný v judikatuře ESLP a na podmínky zákonného omezení v souladu s článkem 52 Listiny.

## 3.1.1. Požadavky oprávněného zásahu podle EÚLP

Zpracování osobních údajů může zasahovat do práva na respektování soukromého života subjektu údajů. Právo na respektování soukromého života však není absolutním právem, ale musí být vyváženo a sladěno s ostatními oprávněnými zájmy, ať již se jedná o zájmy jiných osob (soukromé zájmy), nebo společnosti jako celku (veřejné zájmy).

Podmínky, na základě nichž je zásah státu oprávněný:

### V souladu se zákonem

Podle judikatury ESLP je zásah v souladu se zákonem, je-li založen na ustanovení vnitrostátního práva, které má určité vlastnosti. Právo musí být *„accessible to the persons concerned and foreseeable as to its effects"* [přístupné dotčeným osobám a jeho dopad by měl být předvídatelný].[108] Pravidlo je předvídatelné *„if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct"* [pokud je vyjádřeno dostatečně přesně, aby umožnilo všem jednotlivcům – v případě potřeby pomocí vhodného poradenství – patřičně

108 Rozsudek ESLP [velkého senátu] ze dne 16. února 2000, *Amann proti Švýcarsku,* č. 27798/95, bod 50; viz též rozsudek ESLP ze dne 25. března 1998, *Kopp proti Švýcarsku,* č. 23224/94, bod 55, a rozsudek ESLP ze dne 10. února 2009, *Iordachi a další proti Moldavsku*, č. 25198/02, bod 50.

upravit své chování].[109] *„The degree of precision required of 'the law' in this connection will depend on the particular subject-matter."* [Míra přesnosti vyžadovaná od „práva" v této souvislosti bude záviset na konkrétním předmětu.][110]

Příklad: Ve věci *Rotaru v. Rumunsko* ESLP zjistil, že došlo k porušení článku 8 EÚLP, jelikož rumunské právo povolovalo shromažďování a záznam informací, jež mohou ovlivnit vnitrostátní bezpečnost, a jejich uchovávání v tajných složkách, aniž by stanovilo omezení výkonu těchto pravomocí, což zůstalo na uvážení orgánů.[111] Vnitrostátní právo například nedefinovalo typ informací, které lze zpracovávat, kategorie osob, proti nimž lze opatření týkající se sledování použít, okolnosti, za nichž mohou být taková opatření použita, nebo postup, jež je třeba dodržovat. Na základě těchto nedostatků soud dospěl k závěru, že vnitrostátní právo není v souladu s požadavkem předvídatelnosti podle článku 8 EÚLP a že došlo k porušení uvedeného článku.

Příklad: Ve věci *Taylor-Sabori proti Spojenému království*[112] byl stěžovatel předmětem sledování ze strany policie. Pomocí „klonu" pageru stěžovatele mohla policie zachycovat zprávy, jež mu byly zasílány. Stěžovatel byl poté zatčen a obviněn ze spoluúčasti na dodávkách kontrolované drogy. Část žaloby proti němu se skládala ze zpráv z pageru, které policie přepsala. Avšak v době, kdy probíhal soud stěžovatele, v britském právu neexistovalo žádné ustanovení, které by upravovalo zachycování komunikace přenášené prostřednictvím soukromého telekomunikačního systému. Zásah do jeho práv tudíž nebyl „v souladu se zákonem". ESLP tedy dospěl k závěru, že došlo k porušení článku 8 EÚLP.

109 Rozsudek ESLP [velkého senátu] ze dne 16. února 2000, *Amann proti Švýcarsku,* č. 27798/95, bod 56; viz také rozsudek ESLP ze dne 2. srpna 1984, *Malone proti Spojenému království*, č. 8691/79, bod 66; rozsudek ESLP ze dne 25. března 1983, *Silver a další proti Spojenému království*, č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, bod 88.

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

111 Rozsudek ESLP [velkého senátu] ze dne 4. května 2000, *Rotaru proti Rumunsku,* č. 28341/95, bod 57; viz rovněž rozsudek ESLP ze dne 28. června 2007, *Association for European Integration and Human Rights a Ekimdzhiev proti Bulharsku,* č. 62540/00; rozsudek ESLP ze dne 21. června 2011, *Shimovolos proti Rusku,* č. 30194/09; a rozsudek ESLP ze dne 31. května 2005, *Vetter proti Francii,* č. 59842/00.

112 Rozsudek ESLP ze dne 22. října 2002, *Taylor-Sabori proti Spojenému království*, č. 47114/99.

## Sledování legitimního cíle

Legitimní cíl může být buď cíl v souladu s vyjmenovanými veřejnými zájmy, nebo právy a svobodami druhých.

Příklad: Ve věci *Peck proti Spojenému království*[113] se stěžovatel pokusil o sebevraždu na ulici tak, že si podřezal žíly, nevěděl však, že jej při jeho pokusu natáčí kamera kamerového systému. Poté co jej zachránila policie, která sledovala kamery kamerového systému, policejní orgán předal záznam z kamerového systému médiím, která jej zveřejnila, aniž by zakryla obličej stěžovatele. ESLP shledal, že neexistovaly žádné relevantní nebo dostatečné důvody, jež by ospravedlnily přímé zpřístupnění záznamu orgány veřejnosti bez předchozího souhlasu stěžovatele nebo zakrytí jeho totožnosti. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

## Nezbytné v demokratické společnosti

ESLP uvedl, že *„the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"* [pojem nezbytnost znamená, že zásah je v souladu s naléhavou sociální potřebou, zejména, že je přiměřený sledovanému legitimnímu cíli].[114]

Příklad: Ve věci *Khelili proti Švýcarsku*[115] policie během policejní kontroly zjistila, že stěžovatelka u sebe měla kartičky s textem: *„Nice, pretty woman, late thirties, would like to meet a man to have a drink together or go out from time to time. Tel. no. [...]"* [Milá, pohledná žena středního věku hledá muže za účelem občasných schůzek. Tel. č. [...]. Stěžovatelka tvrdila, že poté, co policie kartičky objevila, zapsali ji do záznamů jako prostitutku, přestože soustavně popírala, že by toto povolání vykonávala. Stěžovatelka žádala, aby z počítačových záznamů policie bylo odstraněno slovo „prostitutka". ESLP v zásadě uznal, že uchovávání osobních údajů osoby z důvodu, že by daná osoba mohla spáchat další přečin, by za určitých okolností mohlo být přiměřené. Nicméně ve věci stěžovatelky se obvinění z nezákonné prostituce zdálo příliš vágní a obecné, nebylo podloženo konkrétními fakty, jelikož nikdy nebyla odsouzena za nezákonnou prostituci,

113 Rozsudek ESLP ze dne 28. ledna 2003, *Peck proti Spojenému království*, č. 44647/98, zejména bod 85.

114 Rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81, bod 58.

115 Rozsudek ESLP ze dne 18. října 2011, *Khelili proti Švýcarsku*, č. 16188/07.

a proto jej nebylo možno považovat za splňující požadavek „naléhavé sociální potřeby“ ve smyslu článku 8 EÚLP. Vzhledem k tomu, že podle soudu prokázání přesnosti údajů uchovávaných o stěžovatelce náleželo orgánům, a vzhledem k závažnosti zásahu do práv stěžovatelky soud rozhodl, že uchovávání slova „prostitutka“ ve spisech policie po několik let nebylo v demokratické společnosti nezbytné. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Leander proti Švédsku*[116] ESLP rozhodl, že tajné prověřování uchazečů o zaměstnání na postech, jež jsou důležité pro národní bezpečnost, nebylo samo o sobě v rozporu s požadavkem na nezbytnost v demokratické společnosti. Na základě zvláštních ochranných opatření stanovených ve vnitrostátním právu pro ochranu zájmů subjektů údajů – např. kontroly prováděné parlamentem a ministrem spravedlnosti (Justitiekanslern) – dospěl ESLP k závěru, že švédský personální kontrolní systém splňuje požadavky čl. 8 odst. 2 EÚLP. Žalovaný stát byl oprávněn s ohledem na velký prostor pro uvážení, jež měl k dispozici, domnívat se, že v případě stěžovatele zájmy národní bezpečnosti převažovaly nad zájmy jednotlivce. Soud dospěl k závěru, že nedošlo k porušení článku 8 EÚLP.

### 3.1.2. Podmínky zákonného omezení podle Listiny EU

Struktura a znění Listiny se liší od EÚLP. Listina nehovoří o zásazích do zaručovaných práv, ale obsahuje ustanovení o omezení(ch) výkonu práv a svobod uznávaných Listinou.

Podle čl. 52 odst. 1 omezení výkonu práv a svobod uznaných Listinou a tím pádem výkonu práva na ochranu údajů, jako je zpracování osobních údajů, jsou přijatelná pouze, jsou-li:

- stanovená zákonem a
- respektují podstatu práva na ochranu údajů a
- jsou nezbytná, při dodržení zásady proporcionality a
- odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.

116 Rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81, body 59 a 67.

Příklady: Ve věci *Volker und Markus Schecke*[117] Soudní dvůr dospěl k závěru, že vyžadováním zveřejňování osobních údajů o všech fyzických osobách, které byly příjemci podpor [určitých zemědělských fondů], aniž by byl činěn rozdíl podle takových relevantních kritérií, jako je doba, po kterou uvedené osoby takové podpory dostávaly, frekvence podpor nebo jejich typ a výše, Rada a Komise překročily meze, které vyžaduje dodržení zásady proporcionality.

Soudní dvůr tudíž shledal, že je nezbytné některá ustanovení nařízení Rady (ES) č. 1290/2005 prohlásit za neplatná a nařízení č. 259/2008 prohlásit za neplatné v celém rozsahu.[118]

Navzdory odlišnému znění, podmínky zákonného zpracování uvedené v čl. 52 odst. 1 Listiny připomínají čl. 8 odst. 2 EÚLP. Podmínky vyjmenované v čl. 52 odst. 1 Listiny je skutečně třeba považovat za významově shodné s podmínkami uvedenými v čl. 8 odst. 2 EÚLP, jelikož čl. 52 odst. 3 Listiny v první větě stanoví, že „[p]okud 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."

Avšak podle poslední věty čl. 52 odst. 3 „[t]oto ustanovení nebrání tomu, aby právo Unie poskytovalo širší ochranu". V kontextu porovnávání čl. 8 odst. 2 EÚLP a první věty čl. 52 odst. 3 se tím pouze rozumí, že podmínky pro oprávněné zásahy podle čl. 8 odst. 2 EÚLP představují minimální požadavky pro zákonná omezení práva na ochranu údajů v souladu s Listinou. Zákonné zpracování osobních údajů tudíž podle práva EU vyžaduje, aby byly splněny alespoň podmínky stanovené v čl. 8 odst. 2 EÚLP; právo EU by však mohlo pro zvláštní případy stanovit další požadavky.

Soulad zásady zákonného zpracování podle práva EU s příslušnými ustanoveními EÚLP dále podporuje čl. 6 odst. 3 SEU, jenž stanoví, že „[z]ákladní práva, která jsou zaručena Evropskou úmluvou o ochraně lidských práv a základních svobod [...] tvoří obecné zásady práva Unie".

117 Rozsudek Soudního dvora ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen,* body 89 a 86.

118 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.

## 3.2. Zásada specifikace a omezení účelu

### Hlavní body

- Účel zpracování údajů musí být zřetelně definován před tím, než je zpracování zahájeno.
- Podle práva EU musí být účel výslovně definován, podle práva RE je tato otázka ponechána na vnitrostátním právu.
- Zpracování za účelem, který není definován, není v souladu s právem v oblasti ochrany údajů.
- Další používání údajů k jinému účelu vyžaduje doplňující právní základ, je-li nový účel zpracování v rozporu s původním.
- Předávání údajů třetím osobám představuje nový účel, jenž vyžaduje doplňující právní základ.

Zásadou specifikace a omezení účelu se v podstatě rozumí, že legitimita zpracování osobních údajů bude záviset na účelu zpracování.[119] Správce je povinen účel specifikovat a jasně prohlásit před zahájením zpracování údajů.[120] **Podle práva EU** tak musí správce učinit prohlášením, jinými slovy oznámením, příslušnému orgánu dozoru nebo alespoň prostřednictvím interní dokumentace, kterou je správce povinen zpřístupnit orgánům dozoru ke kontrole a subjektu údajů k nahlédnutí.

Zpracování osobních údajů pro nedefinované a/nebo neomezené účely je nezákonné.

Každý nový účel pro zpracování údajů musí mít vlastní konkrétní právní základ a není možné spoléhat na skutečnost, že údaje byly původně získány nebo zpracovány za jiným legitimním účelem. Oprávněné zpracování je tedy omezeno na původně stanovený účel a jakýkoli nový účel zpracování bude vyžadovat samostatný nový právní základ. Velmi pečlivě bude zapotřebí zvážit zpřístupnění údajů třetím osobám, jelikož zpřístupnění bude zpravidla představovat nový účel, a tudíž vyžadovat právní základ odlišný od právního základu pro shromažďování údajů.

119 Čl. 2 písm. b) úmluvy č. 108; čl. 6 odst. 1 písm. b) směrnice o ochraně údajů.

120 Viz rovněž pracovní skupina zřízená podle článku 29 (2013), Stanovisko 03/2013 k omezení účelu, WP 203, Brusel, 2. dubna 2013.

Příklad: Letecká společnost shromažďuje údaje od svých cestujících za účelem provádění rezervací, aby se zajistil správný průběh letu. Letecká společnost bude potřebovat údaje o: číslech sedadel cestujících, zvláštních fyzických omezeních, jako jsou potřeby vozíčkáře, a zvláštních stravovacích požadavcích, jako je košer nebo halal jídlo. Pokud je letecká společnost požádána o předání těchto údajů, které jsou obsažené v PNR, imigračním orgánům v místě přistání, jsou tyto údaje pak používány pro účely imigrační kontroly, které se liší od původního účelu shromažďování údajů. Předání těchto údajů imigračnímu orgánu bude proto vyžadovat nový a samostatný právní základ.

Co se týče rozsahu a omezení konkrétního účelu, úmluva č. 108 a směrnice o ochraně údajů se uchylují ke koncepci slučitelnosti: používání údajů pro účely, které jsou slučitelné, je povoleno podle původního právního základu. Co se však rozumí pojmem „slučitelné" není definováno a výklad se může lišit případ od případu.

Příklad: Prodej údajů zákazníků společnosti Sunshine, které získala během řízení vztahů se zákazníky, společnosti působící v oblasti přímého marketingu, Moonlight, která tyto údaje chce použít v marketingových kampaních třetích společností, představuje nový účel, který je neslučitelný s řízením vtahů se zákazníky, tedy s původním účelem společnosti Sunshine pro shromažďování údajů zákazníků. Prodej údajů společnosti Moonlight tudíž vyžaduje vlastní právní základ.

Naproti tomu, když společnost Sunshine použije údaje získané v rámci řízení vztahů se zákazníky pro vlastní marketingové účely, tedy pro zasílání marketingových sdělení týkajících se jejích vlastních produktů vlastním zákazníkům, zpravidla se to akceptuje jako slučitelný účel.

Směrnice o ochraně údajů výslovně uvádí, že „[d]alší zpracování pro historické, statistické nebo vědecké účely není považováno za neslučitelné, pokud členské státy poskytnou vhodná ochranná opatření".[121]

Příklady: Společnost Sunshine shromažďuje a uchovává údaje o svých zákaznících v rámci řízení vztahů se zákazníky. Další používání těchto údajů společností Sunshine pro statistickou analýzu nákupního chování jejích zákazníků je

121 Příkladem takových vnitrostátních ustanovení je rakouský zákon o ochraně údajů (*Datenschutzgesetz*), Věstník rakouských spolkových zákonů I, č. 165/1999, bod 46, v anglickém znění k dispozici na adrese www.dsk.gv.at/DocView.axd?CobId=41936.

přípustné, jelikož statistika představuje slučitelný účel. Žádný dodatečný právní základ, jako je souhlas subjektů údajů, není potřeba.

Pokud by se měly stejné údaje předat třetí osobě, společnosti Starlight, výlučně pro statistické účely, bylo by předání přípustné bez dodatečného právního základu, ale pouze pod podmínkou, že jsou zavedena vhodná ochranná opatření, např. zakrytí totožnosti subjektů údajů, jelikož totožnost pro statistické účely zpravidla není nutná.

## 3.3. Zásady kvality údajů

**Hlavní body**

- Zásady kvality údajů musí být přijaty správcem v průběhu veškerého zpracování.
- Zásada omezené lhůty pro uchovávání údajů usnadňuje odstraňování údajů, jakmile již nejsou potřeba pro účely, k nimž byly shromážděny.
- Výjimky ze zásady omezené lhůty pro uchovávání údajů musí být stanoveny zákonem a vyžadují zvláštní ochranná opatření pro ochranu subjektů údajů.

### 3.3.1. Zásada relevantnosti údajů

Zpracovávají se pouze takové údaje, které jsou „přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány".[122] Kategorie údajů vybraných ke zpracování musí být nezbytné k dosažení stanoveného celkového cíle zpracování a správce by měl shromažďování údajů omezit výlučně na informace, které jsou přímo relevantní konkrétnímu účelu zpracování.

V současné společnosti je u relevantnosti údajů potřeba zvážit ještě další aspekt: využíváním speciální technologie zvyšující ochranu soukromí je někdy možné vyvarovat se používání osobních údajů úplně nebo používat pseudonymizované údaje, přičemž výsledkem je řešení, jež bere ohled na soukromí. To je obzvláště vhodné v rozsáhlejších systémech zpracování.

Příklad: Městská rada nabízí pravidelným uživatelům městské hromadné dopravy čipovou kartu za určitý poplatek. Na kartě je jméno uživatele

122 Čl. 5 písm. c) úmluvy č. 108 a čl. 6 odst. 1 písm. c) směrnice o ochraně údajů.

v písemné podobě na povrchu karty a také v elektronické podobě na čipu. Při každé jízdě autobusem nebo tramvají je třeba kartu přiložit ke čtecím zařízením instalovaným například v autobusech a tramvajích. Data, která zařízení přečte, se automaticky porovnávají s databází obsahující jména osob, které si cestovní kartu zakoupily.

Tento systém optimálně nesplňuje zásadu relevantnosti: ověření, zda je osoba oprávněna využívat hromadnou dopravu, by bylo možné provést bez porovnávání osobních údajů na čipu karty s databází. Postačil by například speciální elektronický obraz, jako je čárový kód, na čipu karty, který by po přiložení ke čtecímu zařízení potvrdil, zda je karta platná, či nikoli. Takový systém by nezaznamenával, kdo použil jaký dopravní prostředek a kdy. Nebyly by shromažďovány žádné osobní údaje, což je optimální řešení ve smyslu zásady relevantnosti, jelikož tato zásada určuje povinnost minimalizovat shromažďování údajů.

## 3.3.2. Zásada přesnosti údajů

Správce uchovávající osobní údaje takové informace nesmí použít, aniž by podnikl kroky k zajištění s přiměřenou jistotou, že jsou údaje přesné a aktuální.

Na povinnost zajistit přesnost údajů je třeba nahlížet v kontextu účelu zpracování údajů.

Příklad: Společnost prodávající nábytek shromáždila údaje o totožnosti a adrese zákazníka, aby mu mohla vystavit fakturu. Šest měsíců později chce tatáž společnost zahájit marketingovou kampaň a kontaktovat bývalé zákazníky. Aby je společnost mohla kontaktovat, chce přístup do národní evidence obyvatel, která bude pravděpodobně obsahovat aktuální adresy, jelikož obyvatelé jsou ze zákona povinni informovat evidenci o své aktuální adrese. Přístup k údajům této evidence je omezen na osoby a subjekty, které mohou předložit oprávněný důvod.

V této situaci společnost nemůže použít argument, že musí zajistit, aby údaje byly přesné a aktuální, aby obhájila, že je oprávněna získat nové údaje o adresách o všech svých bývalých zákaznících z evidence obyvatel. Údaje byly shromážděny při fakturaci, pro tento účel je adresa v okamžiku prodeje relevantní. Neexistuje žádný právní základ pro shromažďování nových údajů o adresách,

jelikož marketing nepředstavuje zájem, který je nadřazen právu na ochranu údajů, a nemůže tudíž být důvodem pro přístup k údajům v evidenci.

V některých případech může být aktualizace uchovávaných údajů též zákonem zakázána, protože účelem uchovávání údajů je v zásadě dokumentace událostí.

Příklad: Zpráva o lékařském zákroku nesmí být měněna, jinými slovy „aktualizována", i kdyby se zjištění uvedená ve zprávě později ukázala jako chybná. Za takových okolností lze provádět pouze dodatky k záznamům ve zprávě, pokud jsou jasně označeny jako později provedené zápisy.

Na druhou stranu existují situace, kdy je pravidelná kontrola přesnosti údajů, včetně jejich aktualizace, naprosto nezbytná vzhledem k případné škodě, kterou by subjekt údajů mohl utrpět, pokud by údaje zůstaly nepřesné.

Příklad: Jestliže někdo chce uzavřít smlouvu s bankovní institucí, banka zpravidla ověřuje úvěruschopnost budoucího klienta. K tomuto účelu existují zvláštní databáze, které obsahují údaje o úvěrové historii soukromých osob. Jestliže taková databáze poskytne o osobě nesprávné nebo zastaralé údaje, tato osoba se může dostat do vážných problémů. Správci takových databází se tudíž musí vynasnažit, aby dodržovali zásadu přesnosti.

Dále, údaje, které se netýkají faktů, ale podezření, jako jsou trestní vyšetřování, mohou být shromažďovány a ukládány, pokud má správce právní základ pro shromažďování takových informací a dostatečný důvod, aby pojal takové podezření.

### 3.3.3. Zásada omezené lhůty pro uchovávání údajů

Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů a podobně čl. 5 písm. e) úmluvy č. 108 vyžadují, aby členské státy zajistily, aby osobní údaje byly „uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány". To znamená, že jakmile jsou účely naplněny, musejí být údaje vymazány.

Ve věci *S. a Marper* ESLP dospěl k závěru, že hlavní zásady příslušných nástrojů Rady Evropy a právní předpisy a praxe ostatních smluvních stran vyžadují, aby uchovávání

údajů bylo přiměřené ve vztahu k účelu shromažďování a omezené v čase, zejména v policejním sektoru.[123]

Časové omezení uchovávání osobních údajů se však použije pouze na údaje uchovávané ve formě, která umožňuje identifikaci subjektů údajů. Zákonného uchovávání údajů, které již nejsou potřeba, by proto mohlo být dosaženo anonymizací údajů nebo pseudonymizací.

Ze zásady omezené lhůty pro uchovávání údajů ve směrnici o ochraně údajů je výslovně vyňato uchovávání údajů pro budoucí vědecké, historické nebo statistické použití.[124] Takové pokračující uchovávání a používání osobních údajů však musí být doplněno zvláštními ochrannými opatřeními podle vnitrostátního práva.

## 3.4. Zásada korektního zpracovávání

**Hlavní body**

- Korektním zpracováním se rozumí průhlednost zpracování, zejména vůči subjektům údajů.
- Správci musí subjekty údajů před zpracováním jejich údajů informovat alespoň o účelu zpracování a o totožnosti a adrese správce.
- Zpracování osobních údajů nesmí být tajné a skryté, pokud to není speciálně povoleno zákonem.
- Subjekty údajů mají právo na přístup ke svým údajům, kdekoli se zpracovávají.

Zásada korektního zpracování upravuje zejména vztah mezi správcem a subjektem údajů.

### 3.4.1. Průhlednost

Tato zásada stanoví správci povinnost informovat subjekty údajů o tom, jak se jejich údaje používají.

123 Rozsudek ESLP ze dne 4. prosince 2008, *S. and Marper proti Spojenému království*, č. 30562/04 a 30566/04; viz rovněž např.: rozsudek ESLP ze dne 13. listopadu 2012, *M.M. proti Spojenému království*, č. 24029/07.

124 Čl. 6 odst. 1 písm. e) směrnice o ochraně údajů.

Příklad: Ve věci *Haralambie proti Rumunsku*[125] stěžovatel požadoval přístup ke složce, kterou o něm vedla organizace tajné služby; jeho žádosti však bylo vyhověno až po pěti letech. ESLP zopakoval, že osoby, o nichž veřejné orgány vedou osobní složky, mají životně důležitý zájem na tom, aby měly k těmto složkám přístup. Orgány byly povinny zajistit efektivní postup pro získání přístupu k takovým informacím. ESLP se domníval, že ani množství předávaných spisů, ani nedostatky archivačního systému nejsou důvodem pro pětileté zpoždění při vyhovění požadavku stěžovatele na přístup k jeho spisu. Orgány stěžovateli neposkytly efektivní a dostupný postup, jehož prostřednictvím by mohl získat přístup ke své osobní složce v přiměřené lhůtě. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Úkony prováděné v rámci zpracování musí být subjektům údajů vysvětleny snadno srozumitelným způsobem, který zajistí, že subjekty chápou, co se s jejich údaji bude dít. Subjekt údajů má rovněž právo na to, získat od správce na žádost informaci o tom, zda se jeho údaje zpracovávají a pokud ano, které.

### 3.4.2. Vytvoření důvěry

Správci by měli subjektům údajů a široké veřejnosti doložit, že budou údaje zpracovávat zákonným a průhledným způsobem. Úkony prováděné v rámci zpracování nesmí být prováděné tajně a neměly by mít nepředvídatelné negativní účinky. Správci by měli zajistit, aby zákazníci, klienti nebo občané byli informov o používání jejich údajů. Správci musejí dále, je-li to možné, jednat způsobem, který pohotově reaguje na přání subjektu údajů, zejména pokud je jeho souhlas právním základem zpracování údajů.

Příklad: Ve věci *K.H. a další proti Slovensku*[126] stěžovatelkami bylo osm romských žen, které byly ošetřovány ve dvou nemocnicích na východním Slovensku během těhotenství a porodu. Poté žádná z nich nemohla i přes opakované pokusy znovu počít dítě. Vnitrostátní soudy nařídily nemocnicím, aby stěžovatelkám a jejich zástupcům povolily přístup k lékařským záznamům a pořízení rukou psaných výňatků, avšak zamítly jejich žádost na pořízení fotokopií dokumentů údajně z důvodu zamezení jejich zneužití. Platné povinnosti států podle článku 8 EÚLP nutně zahrnovaly povinnost poskytnout subjektu údajů kopie složek s jeho údaji. Stát měl stanovit opatření pro pořizování kopií složek osobních

125 Rozsudek ESLP ze dne 27. října 2009, *Haralambie proti Rumunsku*, č. 21737/03.

126 Rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další proti Slovensku*, č. 32881/04.

údajů nebo případně předložit pádné důvody k zamítnutí. Ve věci stěžovatelek vnitrostátní soudy odůvodnily zákaz pořízení kopií lékařských záznamů v zásadě potřebou chránit příslušné informace před zneužitím. ESLP však bylo zatěžko pochopit, jak by stěžovatelky, kterým byl v každém případě poskytnut přístup k jejich úplným lékařským záznamům, mohly zneužít informace, jež se jich týkaly. Riziku takového zneužití bylo navíc možné zabránit jinými prostředky, než odmítnutím stěžovatelkám pořídit kopie záznamů, např. omezením osob, které k záznamům mají přístup. Stát neprokázal existenci dostatečně pádných důvodů k zamítnutí efektivního přístupu stěžovatelek k informacím týkajícím se jejich zdraví. Soud dospěl k závěru, že došlo k porušení článku 8.

Co se týče internetových služeb, funkce systémů zpracování údajů musí subjektům údajů umožňovat skutečně vědět, co se s jejich údaji děje.

Korektním zpracováním se rovněž rozumí, že správci jsou připraveni subjektu údajů poskytnout služby nad rámec povinných zákonem stanovených požadavků, pokud to vyžadují oprávněné zájmy subjektu údajů.

## 3.5. Zásada odpovědnosti

### Hlavní body

- Odpovědnost vyžaduje aktivní provádění opatření ze strany správců na podporu a zabezpečení ochrany údajů v rámci zpracování.
- Správci odpovídají za to, že jimi prováděná zpracování splňují právo v oblasti ochrany údajů.
- Správci by měli být schopni doložit, že dodržují ustanovení o ochraně údajů, subjektům údajů, široké veřejnosti a orgánům dozoru.

Organizace pro hospodářskou spolupráci a rozvoj (OECD) v roce 2013 přijala směrnici o ochraně soukromí, jež zdůraznila, že správci mají důležitou úlohu v zajišťování, aby ochrana údajů fungovala v praxi. Směrnice rozvíjí zásadu odpovědnosti v tom smyslu, že „správce údajů by měl být zodpovědný za dodržování opatření uvádějící výše uvedené [důležité] zásady do praxe.“[127]

127 OECD (2013), Směrnice o ochraně soukromí a přeshraničních tocích osobních údajů, článek 14.

Zatímco v úmluvě č. 108 není odpovědnost správců zmíněna a toto téma je v zásadě ponecháno vnitrostátnímu právu, čl. 6 odst. 2 směrnice o ochraně údajů uvádí, že správce by měl zajistit dodržování zásad týkajících se kvality údajů uvedených v odstavci 1.

Příklad: Příkladem z oblasti právních předpisů pro zdůraznění zásady odpovědnosti je změna[128] směrnice 2002/58/ES o soukromí a elektronických komunikacích z roku 2009. Podle článku 4 pozměněné směrnice, směrnice ukládá povinnost provádět bezpečnostní politiku, jmenovitě „zajistit provádění bezpečnostní politiky týkající se zpracování osobních údajů". Co se týče bezpečnostních ustanovení uvedené směrnice, zákonodárce tedy rozhodl, že je nezbytné zavést výslovný požadavek mít a provádět bezpečnostní politiku.

Podle stanoviska pracovní skupiny zřízené podle článku 29[129] podstata odpovědnosti tkví v povinnosti správce:

- zavést opatření, která by za normálních okolností zaručila, aby při zpracovávání osobních údajů byla dodržována pravidla v oblasti ochrany údajů, a
- mít připravenu dokumentaci, na jejímž základě subjektům údajů a orgánům dozoru doloží, jaká opatření byla přijata pro zajištění dodržování pravidel v oblasti ochrany údajů.

Zásada odpovědnosti tudíž vyžaduje, aby správci aktivně prokazovali dodržování předpisů a aby pouze nečekali na to, až je subjekty údajů nebo orgány dozoru upozorní na nedostatky.

128 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.

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

# 4

# Pravidla evropského práva v oblasti ochrany údajů

| EU | Probíraná témata | RE |
|---|---|---|
| **Pravidla týkající se zákonného zpracování osobních údajů** | | |
| Čl. 7 písm. a) směrnice o ochraně údajů | **Souhlas** | Čl. 3.4 písm. b) a článek 3.6 doporučení o profilování |
| Čl. 7 písm. b) směrnice o ochraně údajů | **(Před)smluvní vztah** | Čl. 3.4 písm. b) doporučení o profilování |
| Čl. 7 písm. c) směrnice o ochraně údajů | **Zákonné povinnosti správce** | Čl. 3.4 písm. a) doporučení o profilování |
| Čl. 7 písm. d) směrnice o ochraně údajů | **Životně důležité zájmy subjektu údajů** | Čl. 3.4 písm. b) doporučení o profilování |
| Čl. 7 písm. e) a čl. 8 odst. 4 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu* | **Veřejný zájem a výkon veřejné moci** | Čl. 3.4 písm. b) doporučení o profilování |
| Čl. 7 písm. f), čl. 8 odst. 2 a čl. 8 odst. 3 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado* | **Oprávněné zájmy druhých** | čl. 3.4 písm. b) doporučení o profilování |
| **Pravidla týkající se zákonného zpracování citlivých údajů** | | |
| Čl. 8 odst. 1 směrnice o ochraně údajů | **Obecný zákaz zpracování** | Článek 6 úmluvy č. 108 |

| EU | Probíraná témata | RE |
|---|---|---|
| Čl. 8 odst. 2–4 směrnice o ochraně údajů | Výjimky z obecného zákazu | Článek 6 úmluvy č. 108 |
| Čl. 8 odst. 5 směrnice o ochraně údajů | Zpracování údajů týkajících se odsouzení (za trestný čin) | Článek 6 úmluvy č. 108 |
| Čl. 8 odst. 7 směrnice o ochraně údajů | Zpracování identifikačních čísel | |
| **Pravidla bezpečného zpracování** | | |
| Článek 17 směrnice o ochraně údajů | Povinnost zajistit bezpečné zpracování | Článek 7 úmluvy č. 108 |
| | | Rozsudek ESLP ze dne 17. července 2008, *I. proti Finsku*, č. 20511/03 |
| Čl. 4 odst. 2 směrnice o soukromí a elektronických komunikacích | Oznamování porušení ochrany údajů | |
| Článek 16 směrnice o ochraně údajů | Povinnost zachovávání důvěrnosti | |
| **Pravidla týkající se průhlednosti zpracování** | | |
| | Průhlednost obecně | Čl. 8 písm. a) úmluvy č. 108 |
| Články 10 a 11 směrnice o ochraně údajů | Informace | Čl. 8 písm. a) úmluvy č. 108 |
| Články 10 a 11 směrnice o ochraně údajů | Výjimky z povinnosti informovat | Článek 9 úmluvy č. 108 |
| Články 18 a 19 směrnice o ochraně údajů | Oznámení | Čl. 9.2 písm. a) doporučení o profilování |
| **Pravidla týkající se podpory dodržování práva** | | |
| Článek 20 směrnice o ochraně údajů | Předběžné kontroly | |
| Čl. 18 odst. 2 směrnice o ochraně údajů | Osoby pověřené ochranou osobních údajů | Článek 8.3 doporučení o profilování |
| Článek 27 směrnice o ochraně údajů | Kodexy chování | |

Zásady jsou nutně obecné. Při jejich uplatňování na konkrétní situace existuje určitý prostor pro výklad a možnost volby prostředků. Podle **práva RE** je ponecháno na stranách úmluvy č. 108, aby tento prostor pro výklad upřesnily. V **právu EU** je situace jiná: pro zavedení ochrany údajů na vnitřním trhu bylo považováno za nezbytné stanovit podrobnější pravidla již na úrovni EU s cílem sblížit míru ochrany údajů

vnitrostátních právních předpisů členských států. Směrnice o ochraně údajů stanoví podle zásad uvedených v článku 6 řadu podrobných pravidel, která musejí být přesně provedena do vnitrostátního práva. Níže uvedené poznámky k podrobným pravidlům v oblasti ochrany údajů na úrovni EU se tudíž týkají převážně práva EU.

## 4.1. Pravidla zákonného zpracování

**Hlavní body**

- Osobní údaje mohou být zpracovávány zákonným způsobem, jestliže:
  - je zpracování založeno na souhlasu subjektu údajů nebo
  - životně důležité zájmy subjektů údajů vyžadují zpracování jejich údajů nebo
  - oprávněné zájmy druhých jsou důvodem ke zpracování, avšak pouze pokud nad nimi nepřeváží zájmy týkající se ochrany základních práv subjektů údajů.
- Zákonné zpracování citlivých údajů upravuje zvláštní, přísnější režim.

Směrnice o ochraně údajů obsahuje dva různé soubory pravidel pro zákonné zpracování údajů: jeden pro údaje, jež nejsou citlivé, v článku 7 a druhý pro citlivé údaje v článku 8.

### 4.1.1. Zákonné zpracování osobních údajů

Kapitola II směrnice 95/46 nazvaná „Obecné podmínky pro zákonnost zpracování osobních údajů" stanoví, že s výhradou výjimek povolených článkem 13 musí být veškeré zpracování osobních údajů v souladu za prvé se zásadami týkajícími se kvality údajů stanovenými v článku 6 směrnice o ochraně údajů a za druhé s jednou ze zásad pro oprávněné zpracování údajů vyjmenovaných v článku 7.[130] To vysvětluje případy, které odůvodňují zpracování osobních údajů.

130 Rozsudek Soudního dvora ze dne 20. května 2003 ve spojených věcech C-465/00, C-138/01 a C-139/01, *Österreichischer Rundfunk a další*, bod 65; rozsudek Soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu*, bod 48; rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*, bod 26.

## Souhlas

**Podle práva RE** souhlas nezmiňuje článek 8 EÚLP ani úmluva č. 108. Je však zmiňován v judikatuře ESLP a v několika doporučeních RE. **Podle práva EU** je souhlas jakožto základ pro oprávněné zpracování údajů pevně stanoven v čl. 7 písm. a) směrnice o ochraně údajů a též výslovně zmíněn v článku 8 Listiny.

## Smluvní vztah

Dalším základem oprávněného zpracování osobních údajů **podle práva EU**, jenž uvádí čl. 7 písm. b) směrnice o ochraně údajů, je, že pokud je „nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran". Toto ustanovení se vztahuje rovněž na předsmluvní vztahy. Například: strana hodlá uzavřít smlouvu, ale ještě tak neučinila, třeba proto, že ještě nebyly dokončeny některé kontroly. Jestliže jedna strana potřebuje za tímto účelem zpracovávat údaje, takové zpracování je zákonné, pokud je třeba „pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu".

**Co se týče práva RE**, čl. 8 odst. 2 EÚLP zmiňuje jako důvod pro zákonný zásah do práva na ochranu údajů „ochranu práv a svobod jiných".

## Zákonné povinnosti správce

**Právo EU** dále výslovně uvádí další zásadu pro oprávněné zpracování údajů, jmenovitě, je-li to „nezbytné pro splnění právní povinnosti, které podléhá správce" (čl. 7 písm. c) směrnice o ochraně údajů). Toto ustanovení se týká správců působících v soukromém sektoru; zákonné povinnosti správců údajů ve veřejném sektoru spadají pod čl. 7 písm. e) směrnice. Existuje mnoho případů, kdy jsou správci v soukromém sektoru ze zákona povinni zpracovávat údaje o druhých, např. lékaři a nemocnice jsou povinni uchovávat údaje o léčbě pacientů po dobu několika let, zaměstnavatelé musejí zpracovávat údaje o svých zaměstnancích z důvodu sociálního zabezpečení a odvádění daní a podniky musejí zpracovávat údaje o svých zákaznících z důvodu odvádění daní.

V souvislosti s povinným předáváním údajů o cestujících leteckými společnostmi zahraničním orgánům imigrační kontroly vyvstala otázka, zda zákonné povinnosti podle *zahraničního* práva mohou být právním základem pro zpracování údajů podle práva EU (této otázce se věnujeme podrobněji v oddílu 6.2).

Zákonné povinnosti správce slouží jako základ pro zákonné zpracování údajů také **podle práva RE**. Jak již bylo zdůrazněno výše, zákonné povinnosti správce v soukromém sektoru představují pouze jeden konkrétní případ oprávněných zájmů druhých, jak uvádí čl. 8 odst. 2 EÚLP. Výše uvedený příklad je proto relevantní také pro právo RE.

## Životně důležité zájmy subjektu údajů

**Podle práva EU** čl. 7 písm. d) směrnice o ochraně údajů stanoví, že zpracování osobních údajů je zákonné, je-li „nezbytné pro zachování životně důležitých zájmů subjektu údajů". Takové zájmy, které jsou úzce spojeny s přežitím subjektu údajů, by mohly představovat základ například pro zákonné používání údajů o zdravotním stavu nebo údajů o pohřešovaných osobách.

**Podle práva RE** článek 8 EÚLP neuvádí životně důležité zájmy subjektu údajů jako důvod pro zákonný zásah do práva na ochranu údajů. Nicméně v některých doporučeních RE, jež doplňují úmluvu č. 108 v určitých oblastech, jsou životně důležité zájmy subjektu údajů jako základ pro zákonné zpracování údajů výslovně uvedeny.[131] Životně důležité zájmy subjektu údajů podle všeho zjevně vyplývají ze souboru důvodů, jež ospravedlňují zpracování údajů: ochrana základních práv by nikdy neměla ohrozit životně důležité zájmy osoby, která je chráněna.

## Veřejný zájem a výkon veřejné moci

Vzhledem k mnoha různým způsobům organizování veřejných záležitostí čl. 7 písm. e) směrnice o ochraně údajů stanoví, že osobní údaje mohou být zákonným způsobem zpracovány, je-li to „nezbytné pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce nebo třetí osoba, které jsou údaje sdělovány […]".[132]

Příklad: Ve věci *Huber proti Německu* pan Huber[133], rakouský státní příslušník pobývající v Německu, požádal Spolkový úřad pro migraci a uprchlíky o výmaz údajů o jeho osobě z centrálního registru cizinců (dále jen „AZR"). Tento registr, který obsahuje osobní údaje o občanech EU, kteří nejsou německými státními příslušníky a kteří pobývají v Německu po dobu delší než tři měsíce, se používá

131 Čl. 3.4 písm. b) doporučení o profilování.

132 Viz též 32. bod odůvodnění směrnice o ochraně údajů.

133 Rozsudek soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu*.

pro statistické účely a také jej používají policejní a justiční orgány při vyšetřování a stíhání trestné činnosti nebo osob, které ohrožují veřejnou bezpečnost. Předkládající soud se dotazoval, zda je zpracování osobních údajů, které se provádí v registru, jako je centrální registr cizinců, do nějž mají přístup také ostatní veřejné orgány, v souladu s právem EU vzhledem k tomu, že pro německé občany žádný takový registr neexistuje.

Soudní dvůr rozhodl za prvé, že podle čl. 7 písm. e) směrnice je zpracování osobních údajů oprávněné, pokud je to nezbytné pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci.

Podle Soudního dvora „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 [...] 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."[134]

Soudní dvůr připomíná, že právo občana Unie na volný pohyb na území členského státu, jehož není státním příslušníkem, není bezpodmínečné, nýbrž s ním mohou být spojena omezení a podmínky stanovené ve Smlouvě, jakož i v předpisech přijatých k jejímu provedení. Pokud je tedy využívání takového registru, jako je AZR, členským státem pro účely podpory orgánů příslušných k provádění právní úpravy v oblasti práva pobytu v zásadě oprávněné, takový registr nesmí obsahovat jiné informace než ty, které jsou za tímto účelem nezbytné. Soudní dvůr dospívá k závěru, že takový systém zpracování osobních údajů je v souladu s právem EU, pokud obsahuje pouze údaje nezbytné k provádění této právní úpravy uvedenými orgány a pokud jeho centralizovaná povaha umožňuje účinnější provádění této právní úpravy. Zda jsou tyto podmínky v této konkrétní věci splněny, musí rozhodnout vnitrostátní soud. Pokud ne, nelze uchovávání a zpracování osobních údajů v registru, jako je AZR, pro statistické účely každopádně považovat za nezbytné ve smyslu čl. 7 písm. e) směrnice 95/46/ES.[135]

A konečně, co se týče otázky používání údajů obsažených v registru pro účely boje proti trestné činnosti, Soudní dvůr rozhodl, že tento cíl „nutně zahrnuje

134 *Tamtéž*, bod 52.

135 *Tamtéž*, body 54, 58, 59, 66–68.

stíhání spáchaných trestných činů a deliktů bez ohledu na státní příslušnost jejich pachatelů". Daný registr neobsahuje osobní údaje týkající se státních příslušníků dotčeného členského státu a toto rozdílné zacházení představuje diskriminaci zakázanou podle článku 18 SFEU. Toto ustanovení, jak jej vykládá Soudní dvůr, tak „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".[136]

Používání osobních údajů orgány činnými ve veřejné sféře upravuje také článek 8 EÚLP.

## Oprávněné zájmy správce nebo třetí osoby

Subjekt údajů není jediným subjektem s oprávněnými zájmy. Čl. 7 písm. f) směrnice o ochraně údajů stanoví, že osobní údaje mohou být zákonným způsobem zpracovávány, je-li to „nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů, které vyžadují ochranu […]".

V následujícím rozsudku Soudní dvůr rozhodoval výslovně o čl. 7 písm. f) směrnice:

Příklad: Ve věci *ASNEF a FECEMD*[137] Soudní dvůr objasnil, že vnitrostátní právo nemůže připojovat dodatečné podmínky k podmínkám uvedeným v čl. 7 písm. f) směrnice o zákonném zpracování údajů. Tato věc se týkala situace, kdy španělský zákon o ochraně údajů obsahoval ustanovení, na jehož základě se mohly jiné soukromé subjekty dovolávat oprávněného zájmu na zpracování osobních údajů pouze, pokud informace již byly uvedeny ve veřejných zdrojích.

Soudní dvůr nejprve konstatoval, že cílem směrnice 95/46 je dosáhnout rovnocenné úrovně ochrany práv a svobod osob v souvislosti se zpracováním osobních údajů ve všech členských státech. Sblížení vnitrostátních právních předpisů použitelných v této oblasti nesmí vést k oslabení ochrany, kterou zajišťují. Naopak musí mít za cíl zajištění vysoké úrovně ochrany v EU.[138] Soudní dvůr

136 *Tamtéž*, body 78 a 81.

137 Rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*.

138 *Tamtéž*, bod 28. Viz 8. a 10. bod odůvodnění směrnice o ochraně údajů.

proto rozhodl, že „z cíle spočívajícího v zajištění rovnocenné úrovně ochrany ve všech členských státech [...] vyplývá, že článek 7 směrnice 95/46 stanoví taxativní a omezující výčet případů, v nichž lze zpracování osobních údajů považovat za zákonné". Navíc „členské státy nemohou doplnit nové zásady pro oprávněné zpracování osobních údajů, obsažené v článku 7 směrnice 95/46 ani upravovat další požadavky, které by pozměnily dosah některé ze šesti zásad zakotvených v tomto článku".[139] Soudní dvůr připustil, že „[p]okud jde o vyvážení požadované ustanovením čl. 7 písm. f) směrnice 95/46, je možné vzít v úvahu okolnost, 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) této 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".

Vzhledem k těmto úvahám dospěl Soudní dvůr k závěru, že „čl. 7 písm. f) směrnice 95/46 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 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".[140]

Podobné formulace lze najít v doporučeních RE. Doporučení o profilování uznává zpracování osobních údajů pro účely profilování jako zákonné, je-li nezbytné pro oprávněné zájmy druhých, *„except where such interests are overridden by the fundamental rights and freedoms of the data subjects"* [s výjimkou případů, kdy nad těmito zájmy převáží zájmy týkající se základních práv a svobod subjektů údajů].[141]

139 Rozsudek Soudního dvora ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado,* body 30–32.

140 *Tamtéž*, body 40, 44, 48 a 49.

141 Čl. 3.4 písm. b) doporučení o profilování.

## 4.1.2. Zákonné zpracování citlivých údajů

**Právo RE** ponechává stanovení náležité ochrany pro používání citlivých údajů na vnitrostátním právu, zatímco **právo EU** v článku 8 směrnice o ochraně údajů stanoví podrobný režim zpracování kategorií údajů, které odhalují: rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost nebo informace týkající se zdraví a sexuálního života. Zpracování citlivých údajů je v zásadě zakázané.[142] Existuje však úplný seznam výjimek z tohoto zákazu, který je uveden v čl. 8 odst. 2 a 3 směrnice. Tyto výjimky zahrnují výslovný souhlas subjektu údajů, životně důležité zájmy subjektu údajů, oprávněné zájmy druhých a veřejný zájem.

Na rozdíl od zpracování údajů, které nejsou citlivé povahy, není smluvní vztah se subjektem údajům pokládán za obecný základ pro oprávněné zpracování citlivých údajů. Pokud se tedy mají citlivé údaje zpracovávat v souvislosti se smlouvou se subjektem údajů, vyžaduje používání těchto údajů kromě souhlasu s uzavřením smlouvy ještě samostatný výslovný souhlas subjektu údajů. Výslovná žádost subjektu údajů o zboží nebo služby, které nutně odhalují citlivé údaje, by nicméně měla být považována za odpovídající výslovnému souhlasu.

Příklad: Jestliže cestující letecké společnosti při rezervaci letenky vyžaduje, aby mu letecká společnost poskytla invalidní vozík a košer jídlo, je letecká společnost oprávněna tyto údaje použít, i když cestující nepodepíše samostatnou doložku o souhlasu uvádějící, že souhlasí s používáním svých údajů odhalujících informace o jeho zdravotním stavu a náboženském vyznání.

### Výslovný souhlas subjektu údajů

První podmínkou zákonného zpracování jakýchkoli údajů, bez ohledu na to, zda se jedná o citlivé údaje či nikoli, je souhlas subjektu údajů. V případě citlivých údajů tento souhlas musí být výslovný. Vnitrostátní právo však může stanovit, že souhlas s používáním citlivých údajů není dostatečným právním základem pro povolení jejich zpracování[143], například kdy ve výjimečných případech jsou se zpracováním spojena neobvyklá rizika pro subjekt údajů.

142 Čl. 8 odst. 1 směrnice o ochraně údajů.

143 *Tamtéž,* čl. 8 odst. 2 písm. a).

V jednom zvláštním případu se jako právní základ pro zpracování citlivých údajů uznává i tichý souhlas: Čl. 8 odst. 2 písm. e) směrnice stanoví, že zpracování není zakázáno, pokud se týká údajů očividně zveřejňovaných subjektem údajů. Toto ustanovení zjevně předpokládá, že jednání subjektu údajů, jímž své údaje zveřejní, musí být vykládáno jako tichý souhlas subjektu údajů s používáním takových údajů.

## Životně důležité zájmy subjektu údajů

Stejně jako v případě osobních údajů mohou být i citlivé údaje zpracovávány z důvodu životně důležitých zájmů subjektu údajů.[144]

Aby zpracování citlivých údajů na tomto základě bylo oprávněné, je nezbytné, aby subjektu údajů nebylo možné položit otázku týkající se jeho rozhodnutí, protože byl například v bezvědomí nebo nepřítomen nebo nemohl být zastižen.

## Oprávněné zájmy druhých

Stejně jako v případě osobních údajů mohou být i pro zpracovávání citlivých údajů oprávněné zájmy druhých. V případě citlivých údajů a v souladu s čl. 8 odst. 2 směrnice o ochraně údajů to však platí pouze v těchto případech:

- kdy je zpracování nezbytné vzhledem k životně důležitým zájmům jiné osoby[145] v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas,

- kdy jsou citlivé údaje relevantní v oblasti pracovního práva, jako jsou údaje o zdravotním stavu, například s ohledem na specificky nebezpečné pracoviště, nebo údaje o náboženském vyznání, například v kontextu dovolených,[146]

- kdy nadace, sdružení nebo jakýkoli jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, zpracovávají údaje o svých členech nebo sponzorech nebo jiných zúčastněných subjektech (takové údaje jsou citlivé, jelikož je pravděpodobné, že odhalí náboženské vyznání, nebo politické přesvědčení dotčených osob),[147]

144 *Tamtéž*, čl. 8 odst. 2 písm. c).

145 *Tamtéž.*

146 *Tamtéž,* čl. 8 odst. 2 písm. b).

147 *Tamtéž,* čl. 8 odst. 2 písm. d).

- kde se citlivé údaje používají v souvislosti se soudním či správním řízením za účelem zjištění, uplatnění nebo obrany právního nároku.[148]

- Kromě toho v souladu s čl. 8 odst. 3 směrnice o ochraně údajů, tato výjimka zahrnuje správu zdravotnických služeb, kde údaje o zdravotním stavu používají poskytovatelé zdravotní péče za účelem lékařského vyšetření a léčby. Existuje zde zvláštní ochranné opatření, kdy osoby jsou považovány za „poskytovatele zdravotní péče" pouze, pokud jsou vázány specifickými profesními povinnostmi k mlčenlivosti.

## Veřejný zájem

Dále v souladu s čl. 8 odst. 4 směrnice o ochraně údajů mohou členské státy stanovit další důvody, pro něž mohou být citlivé údaje zpracovávány, pokud:

- pro zpracování údajů existují důvody významného veřejného zájmu a

- je stanoveno ve vnitrostátních právních předpisech nebo rozhodnutím orgánu dozoru a

- vnitrostátní právní předpisy nebo rozhodnutí orgánu dozoru stanoví nezbytná ochranná opatření, aby byly účinným způsobem chráněny zájmy subjektů údajů.[149]

Vynikajícím příkladem jsou systémy elektronické zdravotní evidence, které mají být v mnoha členských státech zavedeny. Takové systémy umožňují zpřístupňování údajů o zdravotním stavu shromažďovaných poskytovateli zdravotní péče během léčby pacienta ostatním poskytovatelům zdravotní péče tohoto pacienta ve velkém rozsahu, zpravidla na celostátní úrovni.

Pracovní skupina zřízená podle článku 29 dospěla k závěru, že zavádění takových systémů nemůže být provedeno za stávajících právních předpisů týkajících se zpracování údajů o pacientech na základě čl. 8 odst. 3 směrnice o ochraně údajů. Budeme-li však předpokládat, že existence takových systémů elektronické zdravotní evidence představuje významný veřejný zájem, mohla by vycházet z čl. 8 odst. 4 uvedené směrnice, který vyžaduje výslovný právní základ pro vytvoření

148 *Tamtéž,* čl. 8 odst. 2 písm. e).

149 *Tamtéž,* čl. 8 odst. 4.

takových systémů, jenž také obsahuje nezbytná ochranná opatření, která zajistí, že systém bude provozován bezpečně.[150]

## 4.2. Pravidla bezpečnosti zpracování

### Hlavní body

- Pravidla bezpečnosti zpracování zahrnují povinnost správce a zpracovatele přijmout vhodná technická a organizační opatření, aby zamezili neoprávněnému zasahování do zpracování údajů.
- Nezbytnou úroveň zabezpečení údajů určují:
  - bezpečnostní funkce dostupné na trhu pro jakýkoli konkrétní typ zpracování a
  - finanční náklady a
  - citlivá povaha zpracovávaných údajů.
- Bezpečné zpracování údajů dále zabezpečuje obecná povinnost všech osob, správců nebo zpracovatelů, zajistit, aby údaje zůstaly důvěrné.

Povinnost správců a zpracovatelů mít zavedena vhodná opatření pro zajištění zabezpečení údajů je tedy stanovena v **právu RE v oblasti ochrany údajů** i v **právu EU v oblasti ochrany údajů**.

### 4.2.1. Prvky zabezpečení údajů

V souladu s příslušnými ustanoveními **práva EU**:

> *„Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování.“*[151]

Podobné ustanovení existuje v **právu RE**:

150 Pracovní skupina zřízená podle článku 29 (2007), Pracovní dokument věnovaný zpracovávání osobních údajů týkajících se zdraví v elektronických zdravotních záznamech, WP 131, Brusel, 15. února 2007.

151 Čl. 17 odst. 1 směrnice o ochraně údajů.

*„Je třeba učinit vhodná bezpečnostní opatření na ochranu osobních údajů uložených v automatizovaných souborech dat proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, jakož i proti neoprávněnému přístupu, změnám nebo šíření."*[152]

Často se můžeme setkat také s průmyslovými, vnitrostátními a mezinárodními normami, jež byly vypracovány pro bezpečné zpracování údajů. Například Evropský systém osvědčení o ochraně soukromí (EuroPriSe) je projekt eTEN (transevropské telekomunikační sítě) EU, který zkoumá možnosti certifikace produktů, zejména softwaru, jako produktů, jež splňují evropské právo v oblasti ochrany údajů. Evropská agentura pro bezpečnost sítí a informací (ENISA) byla založena s cílem zvyšovat schopnost EU, členských států EU i průmyslu předcházet obtížím v oblasti bezpečnosti sítí a informací, zvládat je a reagovat na ně.[153] ENISA pravidelně zveřejňuje analýzy aktuálních bezpečnostních hrozeb a radí, jak je řešit.

Zabezpečení údajů nelze zajistit jen prostřednictvím správného vybavení – hardwaru a softwaru. Vyžaduje také vhodná interní organizační pravidla. Taková interní pravidla by se v ideálním případě měla týkat těchto otázek:

- pravidelné poskytování informací všem zaměstnancům o pravidlech týkajících se zabezpečení údajů a jejich povinnostech v souladu s právem v oblasti ochrany údajů, zejména ohledně jejich povinností mlčenlivosti,

- jasné rozdělení odpovědností a jasné vytýčení kompetencí v záležitostech zpracování údajů, zejména pokud jde o rozhodnutí zpracovávat osobní údaje a předávat údaje třetím osobám,

- používání osobních údajů pouze v souladu s pokyny kompetentní osoby nebo v souladu s obecně stanovenými pravidly,

- ochrana přístupu do míst a k hardwaru a softwaru správce nebo zpracovatele, včetně kontrol oprávnění k přístupu,

- zajištění pravidel oprávněnosti přístupu k osobním údajům stanovenou a zavedení dokumentace o přístupu,

152 Článek 7 úmluvy č. 108.

153 Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, Úř. věst. 2004 L 77.

- elektronickými prostředky vytvářené automatizované protokoly o přístupu k osobním údajům a pravidelné kontroly takových protokolů interním kontrolním oddělením,

- pečlivě vedená dokumentace pro jiné formy zpřístupnění než je automatizovaný přístup k údajům, aby bylo možné doložit, že nedochází k žádným nezákonným předáváním osobních údajů.

Důležitým prvkem účinných bezpečnostních opatření je rovněž poskytnout zaměstnancům vhodné školení a vzdělání ohledně zabezpečení údajů. Musí být též zavedeny kontrolní postupy, aby bylo zajištěno, že vhodná opatření neexistují pouze na papíře, ale jsou prováděna a fungují v praxi (např. interní nebo externí audity).

Opatření pro zlepšení úrovně bezpečnosti u správce nebo zpracovatele zahrnují nástroje, jako jsou osoby pověřené ochranou osobních údajů, školení o bezpečnosti pro zaměstnance, pravidelné audity, průnikové testy a pečetě kvality.

Příklad: Ve věci *I. proti Finsku*[154] stěžovatelka nebyla schopna prokázat, že k záznamům o jejím zdravotním stavu měli v rozporu se zákonem přístup ostatní zaměstnanci nemocnice, kde pracovala. Vnitrostátní soudy tudíž její žalobu pro porušení jejího práva na ochranu údajů zamítly. ESLP dospěl k závěru, že došlo k porušení článku 8 EÚLP, jelikož evidenční systém nemocnice, v němž byla uchovávána zdravotnická dokumentace *„was such that it was not possible to retroactively clarify the use of patient records as it revealed only the five most recent consultations and that this information was deleted once the file had been returned to the archives“* [byl takový, že nebylo možné zpětně objasnit používání záznamů pacientů, jelikož systém ukazoval pouze pět posledních nahlédnutí a tyto informace byly smazány, jakmile se složka vrátila do archivu]. Pro soud bylo rozhodující, že evidenční systém, jejž nemocnice používala, zjevně nesplňoval zákonné požadavky stanovené ve vnitrostátním právu, což byla skutečnost, jíž vnitrostátní soudy nepřiložily řádnou váhu.

## Oznamování porušení ochrany údajů

Právo v oblasti ochrany údajů v několika evropských zemích zavedlo nový nástroj pro řešení porušení zabezpečení údajů: povinnost poskytovatelů

154 Rozsudek ESLP ze dne 17. července 2008, *I. proti Finsku*, č. 20511/03.

služeb elektronických komunikací oznámit porušení ochrany údajů pravděpodobným poškozeným a orgánům dozoru. Pro poskytovatele telekomunikací je to podle práva EU povinné.[155] Účelem oznámení porušení ochrany údajů subjektům údajů je zamezit škodám: oznámení porušení ochrany údajů a jejich případných důsledků minimalizuje riziko negativních účinků na subjekty údajů. V případech hrubé nedbalosti by poskytovatelům mohly být též uloženy sankce.

Bude nezbytné předem stanovit interní postupy pro účinné řízení a oznamování narušení bezpečnosti osobních údajů, jelikož lhůta týkající se povinnosti vyrozumět subjekty údajů a/nebo orgán dozoru je podle vnitrostátního práva zpravidla poměrně krátká.

## 4.2.2. Důvěrná povaha

**Podle práva EU** bezpečné zpracování údajů dále zabezpečuje obecná povinnost všech osob, správců nebo zpracovatelů, zajistit, aby údaje zůstaly důvěrné.

Příklad: Zaměstnanec pojišťovny na svém pracovišti přijme telefonický hovor od osoby, která tvrdí, že je klientem a požaduje informace týkající se své pojistné smlouvy.

Povinnost zachovávat mlčenlivost o údajích klientů vyžaduje, aby zaměstnanec předtím, než sdělí osobní údaje, přijal alespoň minimální bezpečnostní opatření. To by mohl provést například tak, že klientovi navrhne, že mu zavolá zpět na telefonní číslo uvedené v jeho složce.

Článek 16 směrnice o ochraně údajů se týká důvěrné povahy pouze v rámci vztahu správce–zpracovatel. Povinnost správců zachovávat důvěrnost údajů v tom smyslu, zda je mohou či nemohou sdělovat třetím osobám, upravují články 7 a 8 směrnice.

Povinnost zachovávat důvěrnost se nevztahuje na situace, kdy se osoba o údajích dozví ze svého postavení jako soukromé osoby a nikoli jako zaměstnance správce

155 Viz čl. 4 odst. 3) 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, 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; viz též směrnice 2002/58/ES o zpracovávání 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.

nebo zpracovatele. V tomto případě se článek 16 směrnice o ochraně údajů nepoužije, jelikož používání osobních údajů soukromými osobami je z působnosti směrnice ve skutečnosti zcela vyloučeno, pokud takové používání spadá do takzvané výjimky týkající se zpracování pro vlastní potřebu.[156] Výjimkou týkající se zpracování pro vlastní potřebu se rozumí používání osobních údajů „prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností".[157] Od rozhodnutí Soudního dvora ve věci *Bodil Lindqvist*[158] však musí být tato výjimka vykládána úzce, zejména pokud jde o zpřístupňování údajů. Výjimka týkající se zpracování pro vlastní potřebu se nevztahuje zejména na zveřejňování osobních údajů neomezenému počtu příjemců na internetu (více podrobností o této věci naleznete v oddílech 2.1.2, 2.2, 2.3.1 a 6.1).

**Podle práva RE** povinnost zachování důvěrnosti vyplývá z pojmu zabezpečení údajů v článku 7 úmluvy č. 108, který upravuje zabezpečení údajů.

Pro zpracovatele se zachováním důvěrnosti rozumí, že mohou používat osobní údaje jim svěřené správcem výlučně v souladu s pokyny správce. Pro zaměstnance správce nebo zpracovatele povinnost zachování důvěrnosti vyžaduje, aby osobní údaje používali pouze v souladu s pokyny příslušných nadřízených.

Povinnost zachování důvěrnosti musí být součástí jakékoli smlouvy mezi správci a jejich zpracovateli. Správci a zpracovatelé dále musí přijmout zvláštní opatření, aby pro své zaměstnance stanovili zákonnou povinnost zachování důvěrnosti, což se zpravidla provádí začleněním doložek o zachování mlčenlivosti do pracovní smlouvy zaměstnance.

Porušení pracovních povinností zachování důvěrnosti je v mnoha členských státech EU a stranách úmluvy č. 108 trestným činem podle trestního práva.

156 2. odrážka čl. 3 odst. 2 směrnice o ochraně údajů.

157 *Tamtéž.*

158 Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*.

## 4.3. Pravidla týkající se průhlednosti zpracování

### Hlavní body

- Před zahájením zpracování osobních údajů musí správce přinejmenším informovat subjekty údajů o totožnosti správce a účelu zpracování údajů, pokud s nimi subjekt údajů již nebyl seznámen.
- Jsou-li údaje shromažďovány od třetích osob, povinnost poskytnout informace se nepoužije, jestliže:
  - je zpracování údajů stanoveno ze zákona nebo
  - informování subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí.
- Před zahájením zpracování údajů musí správce dále:
  - vyrozumět orgán dozoru o plánovaném zpracování nebo
  - nechat zpracování interně dokumentovat nezávislou osobou pověřenou ochranou osobních údajů, pokud vnitrostátní právo takový postup stanoví.

Zásada korektního zpracování vyžaduje průhlednost zpracování. **Právo RE** v tomto ohledu stanoví, že každé osobě musí být umožněno zjistit existenci souboru zpracovávaných osobních údajů, jeho účel a odpovědného správce.[159] Stanovení způsobu, jak toho dosáhnout, je ponecháno vnitrostátnímu právu. **Právo EU** je konkrétnější a průhlednost pro subjekty údajů zajišťuje prostřednictvím povinnosti správce informovat subjekt údajů pro širokou veřejnost prostřednictvím oznámení.

Podle obou právních systémů mohou ve vnitrostátním právu existovat výjimky a omezení povinností zajišťování průhlednosti, pokud takové omezení představuje nezbytné opatření pro ochranu určitých veřejných zájmů nebo pro ochranu subjektu údajů či práv a svobod druhých, pokud je to nezbytné v demokratické společnosti.[160] Takové výjimky mohou být například nezbytné v souvislosti s vyšetřováním trestných činů, ale mohou být oprávněné i v jiných situacích.

159 Čl. 8 písm. a) úmluvy č. 108.

160 *Tamtéž*, čl. 9 odst. 2 a čl. 13 odst. 1 směrnice o ochraně údajů.

### 4.3.1. Informační povinnost

**Podle práva RE i podle práva EU** jsou správci zpracování povinni předem informovat subjekt údajů o zpracování, jež hodlají provést.[161] Tato povinnost nezávisí na žádosti ze strany subjektu údajů, nýbrž musí být proaktivně dodržována správcem bez ohledu na to, zda subjekt údajů projeví o informace zájem či nikoli.

#### Obsah informací

Informace musí zahrnovat účel zpracování i totožnost a kontaktní údaje správce.[162] Směrnice o ochraně údajů vyžaduje poskytování doplňujících informací, pokud jsou „nezbytné pro zajištění řádného zpracování údajů vůči subjektu údajů, s ohledem na zvláštní okolnosti, za jakých jsou údaje shromažďovány". Články 10 a 11 této směrnice mimo jiné vymezují kategorie zpracovávaných údajů a příjemce takových údajů i existenci práva na přístup k údajům a práva na jejich opravu. V případě shromažďování údajů od subjektů údajů by měly informace jasně uvádět, zda jsou odpovědi na otázky povinné nebo dobrovolné i případné důsledky neposkytnutí odpovědi.[163]

Z pohledu **práva RE** lze poskytování takových informací považovat za osvědčený postup v souladu se zásadou korektního zpracování údajů a je v tomto rozsahu též součástí práva RE.

Zásada korektního zpracování vyžaduje, aby informace byly pro subjekty údajů snadno srozumitelné. Informace musí být formulovány způsobem, který je vhodný pro příjemce informací. Je třeba použít odlišnou úroveň a typ vyjadřování v závislosti na tom, zda předpokládanými příjemci informací jsou například dospělí nebo děti, široká veřejnost nebo zástupci vědecké obce.

Některé subjekty údajů budou vyžadovat pouze kusé informace o tom, jak a proč se jejich údaje zpracovávají, zatímco jiní budou chtít podrobné vysvětlení. Otázkou, jak zajistit rovnováhu s ohledem na tento aspekt korektního informování, se zabývá pracovní skupina zřízená podle článku 29 ve svém stanovisku, které podporuje myšlenku takzvaných víceúrovňových sdělení[164], na základě kterých se subjekt údajů může rozhodnout, jakou úroveň podrobností upřednostňuje.

161 Čl. 8 písm. a) úmluvy č. 108 a články 10 a 11 směrnice o ochraně údajů.

162 Čl. 8 písm. a) úmluvy č. 108 a čl. 10 písm. a) a b) směrnice o ochraně údajů.

163 Čl. 10 písm. c) směrnice o ochraně údajů.

164 Pracovní skupina zřízená podle článku 29 (2004), Stanovisko 10/2004 k harmonizovanějším ustanovením pro poskytování informací, WP 100, Brusel, 25. listopadu 2004.

## Lhůta pro poskytnutí informací

Směrnice o ochraně údajů obsahuje mírně odlišná ustanovení ohledně toho, kdy mají být informace poskytnuty, v závislosti na tom, zda se údaje shromažďují od subjektu údajů (článek 10) nebo od třetí osoby (článek 11). Pokud se údaje shromažďují od subjektu údajů, musí být informace poskytnuty nejpozději v okamžiku shromažďování. Pokud se údaje shromažďují od třetích osob, musí být informace poskytnuty nejpozději buď poté, co správce údaje zaznamená, nebo před jejich prvním sdělením třetí osobě.

## Výjimky z informační povinnosti

**Podle práva EU** existuje obecná výjimka z povinnosti informovat subjekt údajů, pokud subjekt údajů již s informacemi byl seznámen.[165] To se týká situací, kdy subjekt údajů již podle okolností daného případu ví, že jeho údaje bude zpracovávat určitý správce za určitým účelem.

Článek 11 směrnice, který se týká povinnosti informovat subjekt údajů v případě, kdy údaje nebyly získány od něj, též stanoví, že tato povinnost neexistuje zejména u zpracování pro účely statistiky nebo historických či vědeckých výzkumů, kde:

- informování subjektu údajů není možné nebo
- by vyžadovalo neúměrné úsilí nebo
- pokud právní předpisy výslovně upravují zaznamenávání nebo sdělování údajů.[166]

Pouze čl. 11 odst. 2 směrnice o ochraně údajů stanoví, že subjekty údajů nemusí být o zpracování údajů informovány, pokud takové zpracování upravují právní předpisy. Na základě všeobecného právního předpokladu, že subjekty práva jsou s právem seznámeny, by bylo možné namítat, že pokud jsou údaje shromažďovány podle článku 10 směrnice, subjekt údajů má potřebné informace. Ovšem vzhledem k tomu, že znalost práva je pouhým předpokladem, zásada korektního zpracování by v souladu s článkem 10 vyžadovala, aby subjekt údajů byl informován i tehdy, pokud je zpracování stanoveno zákonem, zejména proto, že informování subjektu

165 Článek 10 a čl. 11 odst. 1 směrnice o ochraně údajů.

166 *Tamtéž*, 40. bod odůvodnění a čl. 11 odst. 2).

údajů není zvláště zatěžující, když jsou údaje shromažďovány přímo od subjektu údajů.

**Co se týče práva RE**, úmluva č. 108 výslovně stanoví výjimky ze svého článku 8. Výjimky stanovené v článcích 10 a 11 směrnice o ochraně údajů lze opět chápat jako příklady správné praxe pro výjimky podle článku 9 úmluvy č. 108.

### Různé způsoby informování subjektů údajů

Ideálním způsobem informování subjektů údajů by bylo ústně či písemně oslovit každý jednotlivý subjekt údajů. Jestliže se údaje shromažďují od subjektu údajů, mělo by být jejich informování provedeno společně se shromažďováním. Ovšem zejména při shromažďování údajů od třetích osob lze informace vzhledem ke zjevným praktickým potížím kontaktovat subjekty údajů osobně poskytnout prostřednictvím vhodného zveřejnění informací.

Jedním z nejúčinnějších způsobů informování subjektů údajů jsou vhodné informační doložky na domovské webové stránce správce, jako jsou například zásady pro ochranu soukromí platné na těchto stránkách. Významná část obyvatel však internet nepoužívá a zásady informování určité společnosti či veřejného orgánu by to měly zohlednit.

## 4.3.2. Oznámení

Vnitrostátní právo může správcům uložit povinnost oznámit příslušný orgán dozoru nad zpracováním osobníchúdajů, jež provádějí, aby bylo možné je zveřejnit. Případně může vnitrostátní právo stanovit, že správci mohou určit osobu pověřenou ochranou osobních údajů, která je zejména pověřena vést seznam zpracování provedených správcem.[167] Tento interní seznam musí být na žádost zpřístupněn veřejnosti.

Příklad: Oznámení i dokumentace vedená interní osobou pověřenou ochranou osobních údajů musí popisovat hlavní prvky dotčeného zpracování údajů. To zahrnuje informace o správci, účelu zpracování, právním základu zpracování, kategoriích zpracovávaných údajů, pravděpodobných třetích příjemcích, a zda se předpokládá předávání údajů do zahraničí, a pokud ano, kam.

167 *Tamtéž*, druhá odrážka čl. 18 odst. 2.

Zveřejňování oznámení orgánem dozoru musí mít formu zvláštního rejstříku. Aby byl tento účel splněn, měl by být přístup do tohoto rejstříku snadný a bezplatný. Totéž platí pro dokumentaci vedenou osobou,kterou správce pověřil ochranou osobních údajů.

Vnitrostátní právo může stanovit výjimky z oznamovací povinnosti vůči příslušnému orgánu dozoru, nebo ustanovení interní osoby pověřené ochranou údajů v souvislosti se zpracováními, u nichž není pravděpodobné, že by představovala zvláštní riziko pro subjekty údajů; tyto jsou uvedeny v čl. 18 odst. 2 směrnice o ochraně údajů.[168]

## 4.4. Pravidla týkající se podpory dodržování práva

**Hlavní body**

- V rámci rozvoje zásady odpovědnosti směrnice o ochraně údajů uvádí několik nástrojů pro podporu dodržování práva:
  - předběžné kontroly plánovaných zpracování ze strany vnitrostátního orgánu dozoru,
  - osoby pověřené ochranou osobních údajů, které správci poskytnou speciální odborné znalosti v oblasti ochrany údajů,
  - kodexy chování, jež stanoví platná pravidla pro ochranu údajů a jež se použijí v pobočce společnosti, zejména podniku.
- Právo RE navrhuje podobné nástroje pro podporu dodržování práva ve svém doporučení o profilování.

### 4.4.1. Předběžné kontroly

V souladu s článkem 20 směrnice o ochraně údajů je orgán dozoru povinen prošetřit zpracování, která by mohla představovat zvláštní rizika z hlediska práv a svobod subjektů údajů – buď v důsledku účelu, nebo okolností zpracování – před jejich započetím. Vnitrostátní právo musí stanovit, jaká zpracování podléhají předběžné kontrole. Výsledkem takového šetření může být zákaz zpracování nebo příkaz změnit

168 *Tamtéž*, první odrážka čl. 18 odst. 2.

prvky navrhované koncepce zpracování. Cílem článku 20 směrnice je zajistit, aby zpracování, které je zbytečně riskantní, nebylo ani započato, jelikož orgán dozoru je oprávněn takové zpracování zakázat. Předpokladem k tomu, aby byl tento mechanismus účinný, je skutečné dodržování oznamovací povinnosti vůči orgánu dozoru. Aby bylo zajištěno, že správci svoji oznamovací povinnost plní, potřebují orgány dozoru donucovací pravomoci, jako je například možnost správcům ukládat sankce.

Příklad: Jestliže společnost provádí zpracování údajů, která podle vnitrostátního práva podléhají předběžné kontrole, musí předložit dokumentaci o plánovaných zpracováních orgánu dozoru. Společnost není oprávněna započít zpracování dříve, než obdrží kladné vyjádření od orgánu dozoru.

V některých členských státech vnitrostátní právo případně stanoví, že zpracování mohou být zahájena, pokud se orgán dozoru nevyjádří v určité lhůtě, například tří měsíců.

## 4.4.2. Osoby pověřené ochranou osobních údajů

Směrnice o ochraně osobních údajů umožňuje, aby vnitrostátní právo stanovilo, že správci mohou určit zaměstnance, který bude plnit úlohu osoby pověřené ochranou osobních údajů.[169] Smyslem zavedení takového postupu je zajistit, že zpracování nemohou poškodit práva a svobody subjektů údajů.[170]

Příklad: V Německu jsou podle čl. 4f odst. 1 spolkového zákona o ochraně údajů (*Bundesdatenschutzgesetz*) společnosti v soukromém vlastnictví povinny určit osobu pověřenou ochranou osobních údajů, jestliže pro automatizované zpracování osobních údajů zaměstnávají 10 či více osob v trvalém pracovním poměru.

Aby zavedená funkce mohla stanovený cíl plnit, je zapotřebí, aby tato pozice měla určitou míru nezávislosti v rámci organizace správce osobních údajů, jak výslovně stanoví směrnice. Rovněž by byla nezbytná účinná pracovní práva, jež by takového zaměstnance chránila například před neoprávněným propuštěním, aby bylo podpořeno účinné fungování té zavedené pozice.

169 *Tamtéž*, druhá odrážka čl. 18 odst. 2.

170 *Tamtéž*.

Za účelem podpory dodržování vnitrostátního práva v oblasti ochrany údajů byl koncept interní osoby pověřené ochranou osobních údajů v organizaci jejich správce přijat též v některých doporučeních RE.[171]

## 4.4.3. Kodexy chování

Na podporu dodržování práva mohou podnikatelská a jiná odvětví vypracovat podrobná pravidla upravující jejich typické aktivity v rámci zpracování údajů, a tak kodifikovat osvědčené postupy. Odborné znalosti členů odvětví pomohou při hledání řešení, která jsou praktická, a tudíž je pravděpodobné, že budou dodržována. Proto se členské státy i Evropská komise vyzývají, aby podporovaly vypracování kodexů chování, jež přispějí k řádnému provádění vnitrostátních ustanovení přijatých členskými státy v souladu se směrnicí, přičemž zohlední specifické rysy různých odvětví.[172]

Aby bylo zajištěno, že tyto kodexy chování splňují vnitrostátní předpisy přijaté v souladu se směrnicí o ochraně údajů, musí členské státy zavést postup pro jejich hodnocení. Tento postup by zpravidla vyžadoval zapojení vnitrostátního orgánu, profesních sdružení a dalších orgánů zastupujících jiné kategorie správců.[173]

Návrhy kodexů Společenství, jakož i změny či prodloužení platnosti stávajících kodexů Společenství, mohou být předloženy k posouzení pracovní skupině zřízené podle článku 29. Evropská komise by měla zajistit vhodné zveřejnění kodexů, které tato pracovní skupina schválila.[174]

Příklad: Federace evropského přímého marketingu (FEDMA) vypracovala evropský kodex chování pro používání osobních údajů v přímém marketingu. Kodex byl úspěšně předložen pracovní skupině zřízené podle článku 29. V roce 2010 byla připojena příloha týkající se elektronických sdělení v přímém marketingu.[175]

171 Viz např. čl. 8.3 doporučení o profilování.

172 Viz čl. 27 odst. 1 směrnice o ochraně údajů.

173 *Tamtéž,* čl. 27 odst. 2.

174 *Tamtéž,* čl. 27 odst. 3.

175 Pracovní skupina zřízená podle článku 29 (2010), Stanovisko 4/2010 k evropskému kodexu chování FEDMA pro používání osobních údajů v přímém marketingu, WP 174, Brusel, 13. července 2010.

# 5

# Práva subjektů údajů a jejich prosazování

| EU | Probíraná témata | RE |
|---|---|---|
| **Právo na přístup** | | |
| Článek 12 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 7. května 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer* | **Právo na přístup k vlastním údajům** | Čl. 8 písm. b) úmluvy č. 108 |
| | **Právo na opravu, výmaz (likvidace) nebo blokování** | Čl. 8 písm. c) úmluvy č. 108<br>Rozsudek ESLP ze dne 18. listopadu 2008, *Cemalettin Canli proti Turecku,* č. 22427/04<br>Rozsudek ESLP ze dne 6. června 2006, *Segerstedt-Wiberg a další proti Švédsku,* č. 62332/00<br>Rozsudek ESLP ze dne 27. dubna 2010, *Ciubotaru proti Moldavsku,* č. 27138/04 |
| **Právo vznést námitku** | | |
| Čl. 14 odst. 1 písm. a) směrnice o ochraně údajů | **Právo vznést námitku související s osobní situací subjektu údajů** | Článek 5.3 doporučení o profilování |
| Čl. 14 odst. 1 písm. b) směrnice o ochraně údajů | **Právo vznést námitku proti dalšímu používání údajů pro marketingové účely** | Článek 4.1 doporučení týkající se přímého marketingu |

| EU | Probíraná témata | RE |
|---|---|---|
| Článek 15 směrnice o ochraně údajů | **Právo vznést námitku proti automatizovaným rozhodnutím** | Článek 5.5 doporučení o profilování |
| **Nezávislý dohled** | | |
| Čl. 8 odst. 3 Listiny<br>Článek 28 směrnice o ochraně údajů<br>Kapitola V nařízení o ochraně údajů zpracovávaných institucemi EU<br>Nařízení o ochraně údajů<br>Rozsudek Soudního dvora ze dne 9. března 2010, C-518/07, *Evropská komise proti Spolkové republice Německo*<br>Rozsudek Soudního dvora ze dne 16. října 2012, C-614/10, *Evropská komise proti Rakouské republice*<br>Rozsudek Soudního dvora ze dne 8. dubna 2014, C-288/12, *Evropská komise proti Maďarsku* | **Vnitrostátní orgány dozoru** | Článek 1 dodatkového protokolu k úmluvě č. 108 |
| **Opravné prostředky a sankce** | | |
| Článek 12 směrnice o ochraně údajů | **Žádost podaná správci** | Čl. 8 písm. b) úmluvy č. 108 |
| Čl. 28 odst. 4 směrnice o ochraně údajů<br>Čl. 32 odst. 2 nařízení o ochraně údajů zpracovávaných institucemi EU | **Žádosti podané orgánu dozoru** | Čl. 1 odst. 2 písm. b) dodatkového protokolu k úmluvě č. 108 |
| Článek 47 Listiny | **Soudy (obecně)** | Článek 13 EÚLP |
| Čl. 28 odst. 3 směrnice o ochraně údajů | **Vnitrostátní soudy** | Čl. 1 odst. 4 dodatkového protokolu k úmluvě č. 108 |
| Čl. 263 odst. 4 SFEU<br>Čl. 32 odst. 1 nařízení o ochraně údajů zpracovávaných institucemi EU<br>Článek 267 SFEU | **Soudní dvůr** | |
| | **ESLP** | Článek 34 EÚLP |

| EU | Probíraná témata | RE |
|---|---|---|
| **Opravné prostředky a sankce** | | |
| Článek 47 Listiny<br>Články 22 a 23 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 10. dubna 1984, C-14/83, *Sabine von Kolson a Elisabeth Kamann proti Land Nordrhein-Westfalen*<br>Rozsudek Soudního dvora ze dne 26. února 1986, C-152/84, *M.H. Marshall proti Southampton and South-West Hampshire Area Health Authority* | **V případě porušení vnitrostátních právních předpisů o ochraně údajů** | Článek 13 EÚLP (pouze členské státy RE)<br>Článek 10 úmluvy č. 108<br>Rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, č. 2872/02<br>Rozsudek ESLP ze dne 25. listopadu 2008, *Biriuk proti Litvě*, č. 23373/03 |
| Články 34 a 49 nařízení o ochraně údajů zpracovávaných institucemi EU<br>Rozsudek Soudního dvora ze dne 29. června 2010, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd* | **V případě porušení práva EU institucemi a orgány EU** | |

Účinnost právních předpisů obecně a konkrétně práv subjektů údajů do velké míry závisí na existenci vhodných mechanismů pro jejich prosazování. V evropském právu v oblasti ochrany údajů musí být subjekt údajů posílen vnitrostátním právem, aby mohl chránit své údaje. Vnitrostátní právo musí také zřizovat nezávislé orgány dozoru, které budou subjektům údajů nápomocny při výkonu jejich práv a které budou dohlížet na zpracování osobních údajů. Dále právo na účinnou právní ochranu zaručené v souladu s EÚLP a Listinou vyžaduje, aby každá osoba měla k dispozici soudní opravné prostředky.

## 5.1. Práva subjektů údajů

### Hlavní body

- Každý musí mít v souladu s vnitrostátním právem právo požadovat od jakéhokoli správce osobních údajů informace o tom, zda daný správce zpracovává jeho údaje, či nikoli.
- Subjekty údajů musí být v souladu s vnitrostátním právem právo na:
  - přístup k vlastním údajům u jakéhokoli správce, který takové údaje zpracovává,
  - opravu svých údajů (nebo případně blokování) správcem, jenž jejich údaje zpracovává, pokud jsou údaje nepřesné,

- výmaz případně blokování údajů správcem, pokud správce údaje zpracovává protiprávně.

- Subjekty údajů mají též právo vznést u správců námitku proti:
  - automaticky přijímaným rozhodnutím (za použití osobních údajů zpracovaných výlučně pomocí automatizovaných postupů),
  - zpracování jejich údajů, jestliže vede k nepřiměřeným výsledkům,
  - používání svých údajů pro účely přímého marketingu.

### 5.1.1. Právo na přístup

**Podle práva EU**, článek 12 směrnice o ochraně údajů stanoví prvky práv subjektů údajů na přístup, včetně práva získat od správce „potvrzení, že údaje, které se ho týkají, jsou či nejsou zpracovávány, jakož i informace týkající se alespoň účelů zpracování, kategorií údajů, na které se zpracování vztahuje, a příjemců nebo kategorií příjemců, kterým jsou údaje sdělovány“ i na „opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí, zejména z důvodů neúplné nebo nepřesné povahy údajů“.

**V právu RE** existují stejná práva, která musí být stanovena vnitrostátním právem (článek 8 úmluvy č. 108). V několika doporučeních RE je používán výraz „přístup“ a různé aspekty práva na přístup jsou popisována a navrhována k provedení do vnitrostátního práva stejným způsobem, jak je uvedeno v odstavci výše.

Podle článku 9 úmluvy č. 108 a článku 13 směrnice o ochraně údajů lze povinnost správců reagovat na žádosti subjektu údajů o přístup omezit z důvodu převažujících právních zájmů druhých. Převažující právní zájmy mohou zahrnovat veřejné zájmy, jako je národní bezpečnost, veřejná bezpečnost a stíhání trestných činů, i soukromé zájmy, které jsou důležitější než zájmy ochrany údajů. Jakékoli výjimky nebo omezení musí být nezbytné v demokratické společnosti a úměrné vzhledem ke sledovanému cíli. Ve výjimečných případech, například z důvodu zdravotních indikací, může sama ochrana subjektu údajů vyžadovat omezení průhlednosti; to se týká zejména omezení práva každého subjektu údajů na přístup.

Pokud se údaje zpracovávají výlučně pro účely vědeckého výzkumu nebo pro statistické účely, směrnice o ochraně údajů povoluje omezit práva k přístupu vnitrostátním právem, avšak musí být zavedena přiměřená právní ochranná opatření. Zejména musí být zajištěno, že v souvislosti s takovým zpracováním údajů nejsou přijímána

žádná opatření nebo rozhodnutí vztahující se na konkrétní osoby a že „prokazatelně neexistuje nebezpečí narušení soukromí subjektu údajů".[176] Podobná ustanovení obsahuje čl. 9 odst. 3 úmluvy č. 108.

## Právo na přístup k vlastním údajům

**Podle práva RE** právo na přístup k vlastním údajům výslovně přiznává článek 8 úmluvy č. 108, ESLP opakovaně rozhodl, že člověk má právo na přístup k informacím o svých osobních údajích uchovávaných nebo zpracovávaných druhými a že toto právo pramení z nutnosti respektovat soukromý život.[177] Ve věci *Leander*[178] ESLP dospěl k závěru, že právo na přístup k osobním údajům uchovávaným veřejnými orgány však může být za určitých okolností omezeno.

**Podle práva EU** je právo na přístup k vlastním údajům výslovně přiznáno v článku 12 směrnice o ochraně údajů a jako základní právo v čl. 8 odst. 2 Listiny.

Čl. 12 písm. a) směrnice stanoví, že členské státy zaručí každému subjektu údajů právo na přístup k vlastním osobním údajům a informacím. Každý subjekt údajů má zejména právo od správce získat informaci, zda údaje, které se ho týkají, jsou či nejsou zpracovávány, jakož i informace týkající se alespoň:

- účelů zpracování,
- kategorií údajů, na které se zpracování vztahuje,
- údajů, které jsou předmětem zpracování,
- příjemců nebo kategorií příjemců, kterým jsou údaje zpřístupnovány
- veškerých dostupných informací o původu údajů, které jsou předmětem zpracování,

176 Čl. 13 odst. 2 směrnice o ochraně údajů.

177 Rozsudek ESLP ze dne 7. července 1989, *Gaskin proti Spojenému království*, č. 10454/83; rozsudek ESLP [velkého senátu] ze dne 13. února 2003, *Odièvre proti Francii*, č. 42326/98; rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další proti Slovensku*, č. 32881/04; rozsudek ESLP ze dne 25. září 2012, *Godelli proti Itálii*, č. 33783/09.

178 Rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81.

- v případě automaticky přijímaných rozhodnutí informace o postupu automatického zpracování údajů.

Vnitrostátní právo může stanovit doplňující informace, které má správce poskytovat, například uvedení právního základu povolujícího zpracování údajů.

Příklad: Má-li subjekt údajů přístup k vlastním osobním údajům, může určit, zda jsou přesné či nikoli. Je proto nezbytné, aby byl informován o kategoriích zpracovávaných údajů i o obsahu údajů. Nestačí tedy, aby správce subjektu údajů pouze oznámil, že zpracovává jeho jméno, adresu, datum narození a oblast zájmu. Správce musí subjektu údajů také sdělit, že zpracovává „jméno: N. N.; adresu: 1040 Vienna, Schwarzenbergplatz 11, Rakousko; datum narození: 10. 10. 1974; a oblast zájmu (na základě prohlášení subjektu údajů): klasická hudba". Poslední položka dále obsahuje informace o původu údajů.

Sdělení týkající se údajů, které jsou předmětem zpracování, a veškerých dostupných informací o jejich původu subjektu údajů musí mít srozumitelnou formu, což znamená, že může být třeba, aby správce subjektu údajů podrobněji vysvětlil, co se rozumí zpracováním. Například pouhé uvedení odborných zkratek nebo lékařských termínů v reakci na žádost o přístup zpravidla nebude dostatečné, i kdyby byly uchovávány pouze tyto zkratky nebo termíny.

Informace o původu údajů, které správce zpracovává, musí být poskytnuty v reakci na žádost o přístup, jsou-li dostupné. Toto ustanovení je nutno chápat v souvislosti se zásadami korektního zpracování a odpovědnosti. Správce nesmí zničit informace o původu údajů, aby je nemusel sdělovat, ani nesmí ignorovat běžný standard a uznávané potřeby ohledně dokumentace v oblasti své činnosti. Pokud správce nebude vést záznamy o původu údajů, které jsou předmětem zpracování, zpravidla nebude plnit své povinnosti podle práva na přístup.

Tam, kde se provádějí automatická hodnocení, bude zapotřebí vysvětlit postup hodnocení, včetně konkrétních kritérií, která byla při hodnocení subjektu údajů zohledněna.

Směrnice jasně nestanoví, zda se právo na přístup k informacím týká minulosti a pokud ano, jakého období v minulosti. V tomto ohledu, jak bylo zdůrazněno v judikatuře Soudního dvora, nesmí být právo na přístup k vlastním údajům nepřiměřeně

omezováno časovými lhůtami. Subjektům údajů musí být poskytnuta přiměřená příležitost získat informace o minulých zpracováních údajů.

Příklad: Ve věci *Rijkeboer*[179] byl Soudní dvůr požádán o určení, zda podle čl. 12 písm. a) směrnice může být právo osoby na přístup k informacím o příjemcích osobních údajů, které se jí týkají, omezeno na období jednoho roku předcházejícího její žádosti o přístup k těmto informacím.

Za účelem určení, zda čl. 12 písm. a) směrnice takovou lhůtu povoluje, Soudní dvůr se rozhodl článek vykládat ve světle cílů směrnice. Soudní dvůr nejprve uvedl, že právo na přístup je nutné k tomu, aby byl subjektu údajů umožněn výkon práva na to, aby správce opravil, vymazal nebo zablokoval jeho údaje (čl. 12 písm. b)) nebo oznámil třetím osobám, jimž byly údaje sděleny, veškeré opravy, výmazy nebo blokování (čl. 12 písm. c)). Právo na přístup je též nutné k tomu, aby byl subjektu údajů umožněn výkon práva na námitku proti zpracování jeho osobních údajů (článek 14) nebo práva na soudní ochranu pro případ utrpěné škody (články 22 a 23).

K zajištění užitečného účinku výše uvedených ustanovení Soudní dvůr rozhodl, 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."

## Právo na opravu, výmaz (likvidaci) nebo blokování údajů

„[K]aždá osoba musí mít možnost požívat práva na přístup k údajům, které se jí týkají a které jsou předmětem zpracování, aby se především přesvědčila o jejich přesnosti a o oprávněnosti jejich zpracování."[180] V souladu s těmito zásadami musí subjekty údajů podle vnitrostátního práva mít právo na to, aby správce opravil, vymazal (zlikvidoval) nebo zablokoval jejich údaje, pokud se domnívají, že jejich zpracování nesplňuje ustanovení směrnice, zejména z důvodu nepřesnosti nebo neúplnosti údajů.[181]

179 Rozsudek Soudního dvora ze dne 7. května 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*.

180 41. bod odůvodnění směrnice o ochraně údajů.

181 *Tamtéž,* čl. 12 písm. b).

Příklad: Ve věci *Cemalettin Canli proti Turecku*[182] ESLP shledal, že došlo k porušení článku 8 EÚLP v nesprávné policejní zprávě v trestním řízení.

Stěžovatel se dvakrát účastnil trestního řízení kvůli obvinění ze členství v ilegálních organizacích, avšak nebyl nikdy odsouzen. Když byl stěžovatel opět zatčen a obviněn z dalšího trestného činu, policie předložila trestnímu soudu zprávu s názvem *„informační formulář o dalších trestných činech"*, v níž stěžovatel figuroval jako člen dvou ilegálních organizací. Žádosti stěžovatele, aby byla zpráva a policejní záznamy změněny, nebylo vyhověno. ESLP rozhodl, že informace v policejní zprávě spadaly do působnosti článku 8 EÚLP, jelikož veřejné informace mohou rovněž spadat pod „soukromý život", pokud jsou systematicky shromažďovány a uchovávány ve spisech vedených orgány. Policejní zpráva navíc byla nesprávná a její vypracování a předložení trestnímu soudu nebylo v souladu se zákonem. Soud dospěl k závěru, že došlo k porušení článku 8.

Příklad: Ve věci *Segerstedt-Wiberg a další proti Švédsku*[183] stěžovatelé byli přidruženi k určitým liberálním a komunistickým politickým stranám. Měli podezření, že informace o nich byly zaznamenány do tajných policejních záznamů. ESLP byl ujištěn, že uchovávání dotčených údajů bylo založeno na právním základě a sledovalo legitimní cíl. U několika ze stěžovatelů ESLP shledal, že pokračující uchovávání údajů představovalo nepřiměřený zásah do jejich soukromého života. Například u pana Schmida orgány uchovávaly informaci, že v roce 1969 údajně podporoval násilný odpor proti policejní kontrole během demonstrací. ESLP shledal, že tato informace nemohla sledovat žádný relevantní zájem v oblasti národní bezpečnosti, zejména vzhledem k její historické povaze. ESLP dospěl k závěru, že u čtyř z pěti stěžovatelů došlo k porušení článku 8 EÚLP.

V některých případech bude dostačující, když bude subjekt údajů jednoduše požadovat opravu například ohledně pravopisu jeho jména, změny adresy nebo telefonního čísla. Jestliže se však takové žádosti týkají právní otázky, jako je například právní subjektivita subjektu údajů nebo správné místo bydliště pro doručování právních písemností, nemusí žádosti na opravu dostačovat a správce může mít nárok na požadování důkazů ohledně údajné nepřesnosti. Takové žádosti nesmí pro subjekt údajů představovat nepřiměřené důkazní břemeno, a tak mu bránit v tom, aby jeho

182 Rozsudek ESLP ze dne 18. listopadu 2008, *Cemalettin Canli proti Turecku*, č. 22427/04, body 33, 42 a 43; rozhodnutí ESLP ze dne 7. února 2010, *Dalea proti Francii*, č. 964/07.

183 Rozsudek ESLP ze dne 6. června 2006, *Segerstedt-Wiberg a další proti Švédsku*, č. 62332/00, body 89 a 90; viz rovněž např.: rozsudek ESLP ze dne 18. dubna 2013, *M.K. proti Francii*, č. 19522/09.

údaje byly opraveny. ESLP shledal porušení článku 8 EÚLP v několika případech, kdy stěžovatel nemohl napadnout nepřesnost informací uchovávaných v tajných rejstřících.[184]

Příklad: Ve věci *Ciubotaru proti Moldavsku* stěžovatel nemohl změnit zápis svého etnického původu v úředních záznamech z moldavského na rumunský údajně proto, že svoji žádost neodůvodnil.[185] ESLP se domníval, že je přijatelné, aby státy při zápisu etnické příslušnosti osoby vyžadovaly objektivní důkaz. Pokud je taková žádost založena čistě na subjektivních a nepodložených důvodech, mohou orgány odmítnout. Žádost stěžovatele však nebyla založena pouze na subjektivním vnímání jeho vlastní etnické příslušnosti; byl schopen předložit objektivně ověřitelná spojení s rumunskou etnickou skupinou, jako je jazyk, jméno, empatie a další. Nicméně podle vnitrostátního práva musel stěžovatel předložit důkaz, že jeho rodiče patřili k rumunské etnické skupině. Vzhledem k dějinám Moldavska takový požadavek vytvořil nepřekonatelnou překážku pro zápis jiné etnické příslušnosti, než jakou u rodičů žalobce zaznamenaly sovětské orgány. Jelikož stát znemožnil stěžovateli, aby jeho žádost byla šetřena ve světle objektivně ověřitelných důkazů, nesplnil svoji povinnost zajistit stěžovateli účinné respektování jeho soukromého života. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Během občanskoprávního sporu nebo řízení před veřejným orgánem týkajícího se rozhodnutí, zda jsou údaje správné či nikoli, může subjekt požádat, aby do jeho spisu byla připojena poznámka, že správnost údajů byla napadena a že ještě nebylo vydáno úřední rozhodnutí. Během tohoto období správce údajů nesmí údaje prezentovat jako konečné, zejména třetím osobám.

Žádost subjektu údajů o výmaz (likvidaci) údajů je často založena na tvrzení, že pro zpracování údajů neexistoval právní základ. Tato tvrzení se často objevují, pokud došlo k odvolání souhlasu nebo některé údaje již nejsou potřeba k plnění účelu, kvůli němuž byly shromážděny. Důkazní břemeno, že zpracování údajů je oprávněné, nese správce údajů, jelikož odpovídá za oprávněnost zpracování. V souladu se zásadou odpovědnosti musí být správce schopen kdykoli osvědčit, že existuje řádný oprávněný důvod pro zpracování údajů, jež provádí, v opačném případě musí být zpracování zastaveno.

184 Rozsudek ESLP ze dne 4. května 2000, *Rotaru proti Rumunsku*, č. 28341/95.

185 Rozsudek ESLP ze dne 27. dubna 2010, *Ciubotaru proti Moldavsku*, č. 27138/04, body 51 a 59.

Jestliže je zpracování údajů napadeno z důvodu údajné nesprávnosti údajů nebo jejich nezákonného zpracování, může subjekt údajů v souladu se zásadou korektního zpracování požadovat zablokování sporných údajů. To znamená, že údaje nejsou vymazány (zlikvidovány), ale že je správce nesmí v době blokování používat. To by bylo obzvláště nezbytné tehdy, kdy by pokračující užívání nesprávných nebo nezákonně držených údajů mohlo subjekt údajů poškodit. Vnitrostátní právo by mělo podrobněji stanovit, kdy může povinnost zablokovat užívání údajů vzniknout a jak by měla být vykonávána.

Subjekty údajů mají dále právo získat od správce oznámení veškerých blokování, oprav nebo výmazů třetím osobám, pokud údaje obdržely před těmito zpracováními. Jelikož správce by měl sdělení údajů třetím osobám zdokumentovat, mělo by být možné identifikovat příjemce údajů a požadovat výmaz. Pokud však byly údaje mezitím zveřejněny například na internetu, nemusí být možné zařídit kompletní výmaz údajů, jelikož příjemce údajů nelze najít. V souladu se směrnicí o ochraně údajů je kontaktování příjemců údajů za účelem opravy, výmazu nebo blokování údajů povinné, „pokud se to neukáže jako nemožné nebo to nevyžaduje nepřiměřené úsilí“.[186]

## 5.1.2. Právo vznést námitku

Právo vznést námitku zahrnuje právo vznést námitku proti automatizovaným individuálním rozhodnutím, právo vznést námitku z důvodů souvisejících s osobní situací subjektu údajů a právo nesouhlasit s dalším používáním údajům pro účely přímého marketingu.

### Právo vznést námitku proti automatizovaným individuálním rozhodnutím

Automaticky přijímaná rozhodnutí jsou rozhodnutí přijímaná za použití osobních údajů zpracovaných výlučně pomocí automatizovaných postupů. Jestliže je pravděpodobné, že taková rozhodnutí budou mít značný dopad na životy jednotlivců, jelikož se týkají například úvěruschopnosti, pracovního výkonu, chování nebo spolehlivosti, je zapotřebí zvláštní ochrana, aby se zamezilo nepříznivým důsledkům. Směrnice o ochraně údajů stanoví, že automaticky přijímaná rozhodnutí by neměla rozhodovat o otázkách, které jsou pro jednotlivce důležité, a vyžaduje, aby jednotlivci měli právo na přezkum automaticky přijatého rozhodnutí.[187]

186 Poslední polovina věty čl. 12 písm. c) směrnice o ochraně údajů.

187 *Tamtéž,* čl. 15 odst. 1.

Příklad: Významným praktickým příkladem automaticky přijímaného rozhodnutí je úvěrové bodování. Aby bylo možné rychle rozhodnout o úvěruschopnosti budoucího klienta, shromažďují se od něj určité údaje, jako je zaměstnání a rodinná situace, které se kombinují s údaji o subjektu dostupnými z jiných zdrojů, například z úvěrových informačních systémů. Tyto údaje jsou automaticky doplněny do algoritmu pro výpočet skóre, který vypočítá celkovou hodnotu vyjadřující úvěruschopnost potenciálního klienta. Takto může zaměstnanec společnosti během okamžiku rozhodnout, zda je subjekt údajů přijatelný jako klient nebo ne.

Nicméně podle směrnice členské státy stanoví, že osoba může být subjektem automatizovaného individuálního rozhodnutí, pokud nejde o zájmy subjektu údajů, protože rozhodnutí bylo učiněno v jeho prospěch, nebo pokud jsou jeho zájmy chráněny vhodnými prostředky.[188] Právo na námitku proti automatizovaným rozhodnutím je též zakotveno v **právu RE**, jak je patrné z doporučení o profilování.[189]

## Právo vznést námitku související s osobní situací subjektu údajů

Neexistuje žádné obecné právo subjektů údajů vznést námitku proti zpracování jejich údajů.[190] Čl. 14 písm. a) směrnice o ochraně údajů však subjekty údajů opravňuje vznést námitku z vážných a legitimních důvodů souvisejících s jeho osobní situací. Podobné právo bylo uznáno v doporučení RE o profilování.[191] Cílem těchto ustanovení je nalézt správnou rovnováhu mezi právy subjektu údajů na ochranu údajů a legitimními právy druhých při zpracování údajů subjektu údajů.

Příklad: Banka uchovává údaje o svých klientech, kteří byli v prodlení se splácením půjčky, sedm let. Klient, jehož údaje jsou v této databázi uloženy, požádá o další půjčku. Banka prověří údaje v databázi, zhodnotí finanční situaci a odmítne klientovi půjčku dát. Klient však může vznést námitku proti tomu, aby jeho osobní údaje byly vedeny v databázi a požádat o jejich výmaz (likvidaci), pokud může prokázat, že prodlení s platbou bylo pouze výsledkem pochybení, které bylo okamžitě napraveno, jakmile je zjistil.

188 *Tamtéž,* čl. 15 odst. 2.

189 Čl. 5 odst. 5) doporučení o profilování.

190 Viz rovněž rozsudek ESLP ze dne 27. srpna 1997, *M.S. proti Švédsku*, č. 20837/92, kdy došlo ke zveřejnění zdravotnické dokumentace bez souhlasu nebo možnosti vznést vůči tomu námitku; nebo rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku*, č. 9248/81, nebo rozsudek ESLP ze dne 10. května 2011, *Mosley proti Spojenému království*, č. 48009/08.

191 Čl. 5 odst. 3) doporučení o profilování.

Je-li námitce vyhověno, správce již nemůže dotčené údaje zpracovávat. Zpracování údajů subjektu údajů před podáním námitky však zůstávají legitimní.

### Právo vznést námitku proti dalšímu používání údajů pro účely přímého marketingu

Čl. 14 písm. b) směrnice o ochraně údajů stanoví zvláštní právo subjektu údajů vznést námitku proti používání jeho údajů pro účely přímého marketingu. Takové právo stanoví také doporučení RE týkající se přímého marketingu.[192] Tento druh námitky má být vznesen předtím, než jsou údaje poskytnuty třetím osobám pro účely přímého marketingu. Subjekt údajů musí tudíž mít příležitost vznést námitku předtím, než jsou údaje předány.

## 5.2. Nezávislý dohled

### Hlavní body

- Aby byla zajištěna účinná ochrana údajů, musí být vnitrostátním právem zřízeny nezávislé orgány dozoru.
- Vnitrostátní orgány dozoru musí jednat zcela nezávisle, přičemž jejich nezávislost musí být stanovena v zakládajícím zákoně a musí se odrážet ve zvláštní organizační struktuře orgánu dozoru.
- Orgány dozoru mají zvláštní úkoly, mezi něž mimo jiné patří:
  - sledování a podpora ochrany údajů na vnitrostátní úrovni,
  - poskytování poradenství subjektům údajů a správcům i vládě a veřejnosti obecně,
  - vyšetřování stížností a pomoc subjektům údajů ohledně údajných porušení práv na ochranu údajů,
  - dozor nad správci a zpracovateli,
  - zasáhnout v případě nutnosti prostřednictvím
    - upozornění, napomenutí či dokonce pokutování správců a zpracovatelů,
    - nařízení opravy, blokování nebo výmazu údajů,
    - zákazu zpracování,
  - obrátit se na soud.

192 RE, 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.

Směrnice o ochraně údajů požaduje nezávislý dozor jako důležitý mechanismus pro zajištění účinné ochrany údajů. Směrnice zavedla nástroj pro prosazování ochrany údajů, který v úmluvě č. 108 nebo směrnici OECD o ochraně soukromí nebyl nejprve stanoven.

Vzhledem k tomu, že se ukázalo, že nezávislý dozor je nepostradatelný pro zajištění účinné ochrany údajů, nové ustanovení revidované směrnice OECD o ochraně soukromí přijaté v roce 2013 vyžaduje, aby členské země *„establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis"* [zřídily a vedly orgány pro prosazování ochrany soukromí disponující nezbytným řízením, zdroji a odbornými znalostmi pro účinný výkon svých pravomocí a přijímání objektivních, nestranných a konzistentních rozhodnutí].[193]

Co se týče **práva RE**, dodatkový protokol k úmluvě č. 108 stanoví, že zřízení orgánů dozoru je povinné. Tento nástroj v článku 1 uvádí právní rámec pro nezávislé orgány dozoru, který musí smluvní strany provést do svého vnitrostátního práva. Pro popis úkolů a pravomocí těchto orgánů používá podobné formulace jako směrnice o ochraně údajů. V zásadě by tedy orgány dozoru měly fungovat stejně podle práva EU jako podle práva RE.

**Podle práva EU** byly kompetence a organizační struktura orgánů dozoru poprvé stanoveny v čl. 28 odst. 1 směrnice o ochraně údajů. Nařízením o ochraně údajů zpracovávaných institucemi EU[194] se zřizuje EIOÚ jako orgán dozoru pro zpracování údajů orgány a institucemi EU. Při vymezování úloh a povinností orgánu dozoru toto nařízení čerpá ze zkušeností získaných od vyhlášení směrnice o ochraně údajů.

Nezávislost orgánů pro ochranu údajů zaručují čl. 16 odst. 2 SFEU a čl. 8 odst. 3 Listiny. Zejména posledně jmenované ustanovení vnímá kontrolu nezávislým orgánem jako zásadní prvek základního práva na ochranu údajů. Směrnice o ochraně údajů dále vyžaduje, aby členské státy zřídily orgány dozoru pověřené dohledem nad používání této směrnice a jednající zcela nezávisle.[195] Nejenom, že zákon, který stanoví

193 OECD (2013), Směrnice o ochraně soukromí a přeshraničních tocích osobních údajů, odst. 19 písm. c).

194 Čl. 41–48 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.

195 Poslední věta čl. 28 odst. 1 směrnice o ochraně údajů; čl. 1 odst. 3 dodatkového protokolu k úmluvě č. 108.

zřízení orgánu dozoru, musí obsahovat určitá ustanovení, jež mu výslovně zaručí nezávislost, nezávislost musí prokazovat i specifická organizační struktura orgánu.

V roce 2010 se Soudní dvůr poprvé zabýval otázkou rozsahu požadavku nezávislosti orgánů dozoru pro ochranu údajů.[196] Jeho uvažování dokládají následující případy.

Příklad: Ve věci *Evropská komise proti Německu*[197] se Evropská komise domáhala toho, aby Soudní dvůr určil, že Německo nesprávně provedlo požadavek „úplné nezávislosti" orgánů dozoru pověřených zajistit ochranu údajů, a tím nesplnilo povinnosti, které pro ně vyplývají z čl. 28 odst. 1 směrnice o ochraně údajů. Podle mínění Komise problém spočíval v tom, že Německo podřídilo státnímu dohledu orgány dozoru pověřené dohledem nad zpracováním osobních údajů v neveřejném sektoru v různých spolkových zemích (*Länder*).

Posouzení opodstatněnosti žaloby podle Soudního dvora záviselo na rozsahu požadavku nezávislosti obsaženém v uvedeném ustanovení, a tudíž na výkladu tohoto ustanovení.

Soudní dvůr zdůraznil, že výraz „zcela nezávisle" v čl. 28 odst. 1 směrnice je třeba vykládat na základě skutečného znění uvedeného ustanovení a cílů a uspořádání směrnice o ochraně údajů.[198] Soudní dvůr zdůraznil, že orgány dozoru jsou „strážci" práv souvisejících se zpracováním osobních údajů zakotvených v této směrnici a že jejich zřízení v členských státech je tudíž pokládáno za „zásadní prvek ochrany osob v souvislosti se zpracováním osobních údajů".[199] Soudní dvůr 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 nebo spolkových zemí, a nikoli pouze před vlivem organizací, na které dohlíží."[200]

196 Viz 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 se této otázce věnuje podrobněji ve své zprávě *Ochrana údajů v Evropské unii: úloha vnitrostátních orgánů pro ochranu údajů*, která byla zveřejněna v květnu 2010.

197 Rozsudek Soudního dvora ze dne 9. března 2010, C-518/07, *Evropská komise proti Spolkové republice Německo,* bod 27.

198 *Tamtéž*, body 17 a 29.

199 *Tamtéž*, bod 23.

200 *Tamtéž*, bod 25.

Soudní dvůr též shledal, že výraz „úplná nezávislost" by měl být vykládán ve světle nezávislosti EIOÚ jak definuje nařízení o ochraně údajů zpracovávaných institucemi EU. Jak Soudní dvůr zdůraznil, čl. 44 odst. 2 uvedeného článku vysvětluje pojem nezávislosti dovětkem, že při výkonu své funkce EIOÚ od nikoho nevyžaduje ani nepřijímá pokyny. Tak je vyloučen státní dozor nad nezávislým orgánem dozoru pro ochranu údajů.[201]

Soudní dvůr tedy rozhodl, že německé orgány dozoru na úrovni spolkových zemí pověřené dohledem nad zpracováním údajů neveřejnoprávními organizacemi nebyly dostatečně nezávislé, jelikož podléhaly státnímu dohledu.

Příklad: Ve věci *Evropská komise proti Rakousku* Soudní dvůr poukázal na podobné problémy týkající se funkce některých členů a zaměstnanců rakouského orgánu pro ochranu údajů (komise pro ochranu osobních údajů, DSK).[202] Soud v této věci dospěl k závěru, že rakouské právní předpisy znemožňují rakouskému orgánu pro ochranu údajů vykonávat jeho úkoly zcela nezávisle ve smyslu směrnice o ochraně údajů. Nezávislost rakouského orgánu pro ochranu údajů nebyla dostatečně zaručena, protože pracovníky DSK poskytoval úřad spolkového kancléře, uvedený úřad dohlížel nad DSK a měl právo být neustále informován o její práci.

Příklad: Ve věci *Evropská komise proti Maďarsku*[203] Soudní dvůr 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". Soudní dvůr tedy 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 [...]".

Orgány dozoru mají v souladu s vnitrostátním právem pravomoci a způsobilost:[204]

- poskytovat poradenství správcům a subjektům údajů ve všech záležitostech ochrany údajů,

201 *Tamtéž*, bod 27.

202 Rozsudek Soudního dvora ze dne 16. října 2012, C-614/10, *Evropská komise proti Rakouské republice*, body 59 a 63.

203 Rozsudek Soudního dvora ze dne 8. dubna 2014, C-288/12, *Evropská komise proti Maďarsku*, body 50 a 67.

204 Článek 28 směrnice o ochraně údajů; viz dále článek 1 dodatkového protokolu k úmluvě č. 108.

- provádět šetření týkající se zpracování údajů a příslušným způsobem zasahovat,
- zaslat správcům upozornění nebo napomenutí,
- nařídit opravu, blokování, výmaz nebo likvidaci údajů,
- dočasně nebo trvale zakázat zpracování,
- obrátit se na soud.

Aby orgán dozoru mohl své funkce vykonávat, musí mít přístup ke všem osobním údajům a informacím potřebným pro vyšetřování i přístup do jakýchkoli prostor, kde správce příslušné informace uchovává.

Co se týče řízení a právních důsledků zjištění orgánů dozoru, mezi vnitrostátními jurisdikcemi existují značné rozdíly. Může sahat od doporučení ochránce práv až po okamžitě vykonatelná rozhodnutí. Při analyzování účinnosti opravných prostředků dostupných v určité jurisdikci, musí být nápravné nástroje posuzovány v jejich kontextu.

## 5.3. Opravné prostředky a sankce

### Hlavní body

- V souladu s úmluvou č. 108 i směrnicí o ochraně údajů musí vnitrostátní právo stanovit vhodné opravné prostředky a sankce pro případy porušení práva na ochranu údajů.
  - Právo na účinnou právní ochranu vyžaduje podle práva EU, aby vnitrostátní právo stanovilo soudní opravné prostředky pro případy porušení práv na ochranu údajů bez ohledu na možnost obrátit se na orgán dozoru.
  - Vnitrostátní právo musí stanovit sankce, které jsou účinné, ekvivalentní, přiměřené a odrazující.
- Předtím než se subjekt údajů obrátí na soudy, musí se nejprve obrátit na správce osobních údajů. To, zda je také povinné se před podáním žaloby k soudu nejprve obrátit na orgán dozoru nebo ne, je ponecháno na úpravě vnitrostátním právem.
- Jako poslední možnost a za určitých podmínek subjekty údajů mohou podat žalobu pro porušení práva v oblasti ochrany údajů u ESLP.
- Subjekty údajů se též mohou obrátit na Soudní dvůr, avšak jen ve velmi omezené míře.

Práva podle práva v oblasti ochrany údajů může vykonávat pouze osoba, o jejíž práva se jedná; to bude někdo, kdo minimálně tvrdí, že je subjektem údajů. Takové osoby mohou být při výkonu svých práv zastupovány osobami, které podle vnitrostátního práva splňují nezbytné požadavky. Nezletilé osoby musí zastupovat rodiče nebo poručníci. Před orgány dozoru může osobu též zastupovat sdružení, jehož zákonným cílem je podpora práv na ochranu údajů.

### 5.3.1. Žádosti podané správci

Práva uvedená v oddílu 3.2 musí být nejprve uplatňována vůči správci osobních údajů. Pokud by se subjekt údajů obrátil přímo na vnitrostátní orgán dozoru nebo soud, nepomohlo by to, jelikož orgán by mohl subjektu pouze poradit, aby se nejprve obrátil na správce, a soud by žalobu shledal nepřípustnou. Formální požadavky na právně relevantní žádost podanou správci, zejména to, zda musí mít písemnou formu, či nikoli, by mělo upravovat vnitrostátní právo.

Subjekt, který byl osloven jako správce, musí na žádost reagovat, i když správcem není. Odpověď musí být v každém případě doručena subjektu údajů ve lhůtě stanovené vnitrostátním právem, i pokud obsahuje pouze vyjádření, že o žadateli nejsou zpracovávány žádné údaje. V souladu s ustanoveními čl. 12 písm. a) směrnice o ochraně údajů a čl. 8 písm. b) úmluvy č. 108 musí být žádost vyřízena „bez přílišných průtahů“. Vnitrostátní právo by tudíž mělo stanovit lhůtu pro odpověď, která je dostatečně krátká, přesto však správci umožňuje žádost odpovídajícím způsobem řešit.

Předtím, než subjekt, na nějž se žadatel obrátil jako na správce, na žádost odpoví, musí zjistit totožnost žadatele, aby mohl určit, zda je skutečně osobou, kterou tvrdí, že je, a tak zamezit závažnému porušení důvěrnosti. Pokud požadavky na zjišťování totožnosti konkrétně neupravuje vnitrostátní právo, musí je stanovit správce. Zásada korektního zpracování by však vyžadovala, aby správci nestanovovali příliš náročné podmínky pro uznání identifikace (a pravosti žádosti, o čemž pojednává oddíl 2.1.1)

Vnitrostátní právo musí rovněž upravovat otázku, zda mohou správci předtím, než na žádost odpovědí, požadovat od žadatele uhrazení poplatku či nikoli. Čl. 12 písm. a) směrnice a čl. 8 písm. b) úmluvy č. 108 stanoví, že odpověď na žádost o přístup musí být poskytnuta „bez [...] nadměrných nákladů“. Vnitrostátní právo v mnoha evropských zemích stanoví, že odpovědi na žádosti v souladu s právem v oblasti ochrany údajů musejí být poskytovány zdarma, pokud poskytnutí odpovědi není spojeno s nadměrným a neobvyklým úsilím; naopak správci jsou zpravidla v souladu

s vnitrostátním právem chráněni před zneužíváním práva na získání odpovědi na žádosti.

Jestliže osoba, instituce nebo orgán, na nějž se žadatel obrátí jako na správce, nepopírá, že je správcem, tento subjekt je povinen ve lhůtě stanovené vnitrostátním právem:

- buď žádosti vyhovět a uvědomit žadatele, jak byla žádost vyřízena, nebo
- informovat žadatele, proč jeho žádosti nebude vyhověno.

## 5.3.2. Žádosti podané orgánu dozoru

Pokud osoba, která podala žádost o přístup nebo vznesla námitku u správce, neobdrží včasnou a uspokojivou odpověď, může se s žádostí o pomoc obrátit na vnitrostátní orgán dozoru pro ochranu údajů. Během řízení před orgánem dozoru by mělo být objasněno, zda osoba, instituce nebo orgán, na něž se žadatel obrátil, byly opravdu povinny se žádostí zabývat a zda jejich reakce byla správná a dostačující, či nikoli. Orgán dozoru musí dotčené osobě oznámit výsledek řízení týkající se její žádosti.[205] Právní účinky výsledků řízení před vnitrostátními orgány dozoru závisí na vnitrostátním právu: zda mohou být rozhodnutí orgánu vykonána v souladu se zákonem, tedy zda jejich výkon může prosazovat orgán veřejné moci, nebo zda je nezbytné se odvolat k soudu, pokud se správce rozhodnutím orgánu dozoru neřídí (stanovisko, napomenutí atd.).

V případě, že dojde k údajnému porušení práv na ochranu údajů, jež zaručuje článek 16 SFEU, institucemi nebo orgány EU, může subjekt údajů podat stížnost k EIOÚ[206], nezávislému orgánu dozoru pro ochranu údajů v souladu s nařízením o ochraně údajů zpracovávaných institucemi EU, jež stanoví povinnosti a pravomoci EIOÚ. Jestliže se EIOÚ nevyjádří do šesti měsíců, má se za to, že stížnost byla zamítnuta.

Proti rozhodnutím vnitrostátního orgánu dozoru musí být možné se odvolat k soudu. To platí pro subjekt údajů i pro správce, jakožto účastníky řízení vedenéhoorgánem dozoru.

205 Čl. 28 odst. 4 směrnice o ochraně údajů.

206 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.

Příklad: Komisař pro informace Spojeného království (Information Commissioner) vydal dne 24. července 2013 rozhodnutí, v němž žádal policii v Hertfordshiru, aby přestala používat systém pro sledování registračních značek automobilů, který považoval za nezákonný. Údaje shromažďované pomocí kamer byly uchovávány jak v databázích místní policie, tak v centrální databázi. Fotografie registračních značek byly uchovávány po dobu dvou let a fotografie automobilů po dobu 90 dnů. Komisař rozhodl, že takto rozsáhlé používání kamer a dalších forem sledování nebylo přiměřené problému, který se snažilo řešit.

## 5.3.3. Žaloba podaná k soudu

V souladu se směrnicí o ochraně údajů osoba, která podala žádost správci osobních údajů podle práva v oblasti ochrany údajů a která není spokojena s odpovědí správce, musí být oprávněna podat žalobu k vnitrostátnímu soudu.[207]

To, zda je povinné se před podáním žaloby k soudu nejprve obrátit na orgán dozoru nebo ne, je ponecháno na úpravě vnitrostátním právem. Ve většině případů však pro osoby uplatňující svá práva na ochranu údajů bude výhodnější obrátit se nejprve na orgán dozoru, jelikož vyřizování žádostí o jejich pomoc by mělo být nebyrokratické a bezplatné. Odborný posudek uvedený v rozhodnutí orgánu dozoru (stanovisko, napomenutí atd.) může subjektu údajů rovněž pomoci domáhat se svých práv u soudu.

**Podle práva RE** mohou být porušení práv na ochranu údajů, jichž se údajně dopustila smluvní strana EÚLP na vnitrostátní úrovni a jež zároveň představují porušení článku 8 EÚLP, dále předložena ESLP poté, co byly vyčerpány všechny dostupné vnitrostátní opravné prostředky. Podání žaloby pro porušení článku 8 EÚLP k ESLP musí též splňovat další podmínky přijatelnosti (články 34–37 EÚLP).[208]

Přestože k ESLP lze podat pouze žaloby proti smluvním stranám, nepřímo se mohou týkat rovněž jednání nebo opomenutí soukromých osob, pokud smluvní strana nesplnila své povinnosti podle EÚLP a nezajistila dostatečnou ochranu před porušováním práv na ochranu údajů ve svém vnitrostátním právu.

207 Článek 22 směrnice o ochraně údajů.

208 Čl. 34–37 EÚLP, k dispozici na adrese: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

Příklad: Ve věci *K.U. proti Finsku*[209] si stěžovatel, nezletilý, stěžoval, že o jeho osobě byl zveřejněn inzerát sexuální povahy na internetové seznamce. Poskytovatel služby neodhalil totožnost osoby, která informace zveřejnila, v důsledku povinností zachování důvěrnosti stanovených ve finském právu. Stěžovatel tvrdil, že finské právo nezajišťuje dostatečnou ochranu před takovým jednáním soukromé osoby, která na internet umisťuje inkriminující údaje o stěžovateli. ESLP rozhodl, že nejenom, že je potřeba, aby se státy vyvarovaly svévolných zásahů do soukromých životů jednotlivců, ale mohou být též povinny dodržovat určité povinnosti, jež zahrnují *„the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves"* [přijetí opatření určených k zajištění respektování soukromého života také v oblasti vzájemných vztahů mezi jednotlivci]. Ve věci stěžovatele vyžadovala praktická a účinná ochrana jeho osoby, aby byly podniknuty účinné kroky k identifikaci a stíhání pachatele. Stát však takovou ochranu neposkytoval a soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Köpke proti Německu*[210] byla stěžovatelka podezřelá z krádeže na pracovišti, a proto byla podrobena skrytému sledování pomocí kamerového systému. ESLP dospěl k závěru, že *„nothing to indicate that the domestic authorities failed to strike a fair balance, within their margin of appreciation, between the applicant's right to respect for her private life under Article 8 and both her employer's interest in the protection of its property rights and the public interest in the proper administration of justice"* [nic neukazuje, že by vnitrostátní orgány v rámci svého prostoru pro uvážení nezajistily spravedlivou rovnováhu mezi právem stěžovatelky na respektování jejího soukromého života v souladu s článkem 8 a zájmem zaměstnavatele na ochranu jeho vlastnických práv i veřejným zájmem na řádný výkon spravedlnosti]. Žaloba byla tudíž prohlášena za nepřípustnou.

Jestliže ESLP shledá, že stát, který je smluvní stranou EÚLP porušuje jakákoli z práv chráněná touto úmluvou, je tento stát povinen vykonat rozsudek ESLP. Opatření přijatá v rámci výkonu rozsudku musí nejprve ukončit porušování práv a napravit jeho negativní dopady na stěžovatele v maximální možné míře. Výkon rozsudků může vyžadovat také přijetí obecných opatření, aby szamezilo podobnému porušování práv, jež shledal soud, ať již prostřednictvím změn právních předpisů, judikatury nebo jiných opatření.

209 Rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, č. 2872/02.

210 Rozhodnutí ESLP ze dne 5. října 2010, *Köpke proti Německu*, č. 420/07.

Jestliže soud prohlásí, že byla porušena EÚLP, článek 41 EÚLP stanoví, že může přiznat stěžovateli spravedlivé zadostiučinění na náklady státu, jenž je smluvní stranou EÚLP.

**Podle práva EU**[211] mohou osoby poškozené porušením vnitrostátního práva v oblasti ochrany údajů, které provádí právo EU v oblasti ochrany údajů, v některých případech předložit věc Soudnímu dvoru. Existují dva možné scénáře, jak může žaloba subjektu údajů pro porušení jeho práv na ochranu údajů vést k řízení před Soudním dvorem.

V prvním scénáři by subjekt údajů musel být přímo poškozený správním nebo regulačním aktem EU, který porušuje právo jednotlivce na ochranu údajů. V souladu s čl. 263 odst. 4 SFEU:

> *„každá fyzická nebo právnická osoba může [...] podat žalobu proti aktům, které jsou jí určeny nebo které se jí bezprostředně a osobně dotýkají, jakož i proti právním aktům s obecnou působností, které se jí bezprostředně dotýkají a nevyžadují přijetí prováděcích opatření"*

Osoby poškozené nezákonným zpracováním svých údajů orgánem EU se tak mohou odvolat přímo k Tribunálu Soudního dvora, což je orgán oprávněný rozhodovat v záležitostech nařízení o ochraně údajů zpracovávaných institucemi EU. Přímo k Soudnímu dvoru se lze odvolat také tehdy, pokud je právní situace subjektu přímo ovlivněna právním ustanovením EU.

Druhý scénář se týká pravomoci Soudního dvora rozhodovat o předběžných otázkách v souladu s článkem 267 SFEU.

Subjekty údajů se mohou během vnitrostátního řízení obrátit na vnitrostátní soud a jeho prostřednictvím požádat Soudní dvůr o vysvětlení výkladu Smluv EU a výkladu a platnosti aktů institucí, orgánů, úřadů a agentur EU. Tato vysvětlení se označují jako rozhodnutí o předběžných otázkách. Nejedná se o přímý opravný prostředek pro stěžovatele, ale pomáhá vnitrostátním soudům zaručit, že používají správný výklad práva EU.

211 EU (2007), Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství podepsaná v Lisabonu dne 13. prosince 2007, Úř. věst. 2007 C 306. Viz rovněž konsolidovaná znění Smlouvy o Evropské unii, Úř. věst. 2012 C 326, a SFEU, Úř. věst. 2012 C 326.

Jestliže účastník řízení před vnitrostátními soudy požádá o předložení otázky Soudnímu dvoru, povinnost vyhovět takové žádosti mají pouze vnitrostátní soudy poslední instance, proti jejichž rozhodnutí se již nelze odvolat.

Příklad: Ve věci *Kärntner Landesregierung a další*[212] Verfassungsgerichtshof (rakouský ústavní soud) předložil Soudnímu dvoru otázky týkající se platnosti článků 3 až 9 směrnice 2006/24/ES (*směrnice o uchovávání údajů*) ve světle článků 7, 9 a 11 Listiny a toho, zda určitá ustanovení rakouského spolkového zákona o telekomunikacích, jenž provádí směrnici o uchovávání údajů, jsou neslučitelná s aspekty směrnice o ochraně údajů a nařízení o ochraně údajů zpracovávaných institucemi EU, či nikoli.

Pan Seitlinger, jeden z účastníků řízení před ústavním soudem, uvedl, že používá telefon, internet a e-mail pro pracovní účely i v soukromém životě. Informace, které zasílá a přijímá, jsou tak přenášeny prostřednictvím veřejných telekomunikačních sítí. Podle rakouského zákona o telekomunikacích z roku 2003 má jeho poskytovatel telekomunikačních služeb ze zákona právo shromažďovat a uchovávat údaje o jeho používání sítě. Pan Seitlinger zjistil, že toto shromažďování a uchovávání jeho osobních údajů nebylo v žádném případě nutné pro technické účely předání informace z bodu A do bodu B sítě. Shromažďování a uchovávání těchto údajů nebylo v žádném případě nutné ani pro účely fakturace. Pan Seitlinger rozhodně neposkytl souhlas s takovým používáním svých osobních údajů. Jediným důvodem pro shromažďování a uchovávání všech těchto nadbytečných údajů byl rakouský zákon o telekomunikacích z roku 2003.

Pan Seitlinger tudíž podal žalobu k rakouskému ústavnímu soudu, v níž uvedl, že zákonné povinnosti jeho poskytovatele telekomunikačních služeb porušují jeho základní práva podle článku 8 Listiny EU.

Soudní dvůr rozhoduje pouze o základních prvcích žádosti o předběžné otázce, jež je mu předložena. Rozhodnutí v původní věci přísluší vnitrostátnímu soudu.

Soudní dvůr v zásadě musí odpovědět na dotazy, jež jsou mu předloženy. Nemůže odmítnout rozhodnout o předběžné otázce s odůvodněním, že tato odpověď by nebyla v souvislosti s původní věci ani relevantní ani včasná. Nicméně může odmítnout, pokud je otázka mimo jeho oblast působnosti.

212 Rozsudek Soudního dvora ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a další*.

Konečně, jestliže instituce nebo orgán EU při zpracování osobních údajů údajně porušuje práva na ochranu údajů, jež jsou zaručena článkem 16 SFEU, je subjekt údajů oprávněn věc předložit Tribunálu Soudního dvora (čl. 32 odst. 1 a 4 nařízení o ochraně údajů zpracovávaných institucemi EU). Totéž platí pro rozhodnutí EIOÚ ohledně takových porušení práv (čl. 32 odst. 3 nařízení o ochraně údajů zpracovávaných institucemi EU).

Přestože Tribunál Soudního dvora je oprávněn rozhodovat v záležitostech nařízení o ochraně údajů zpracovávaných institucemi EU, pokud chce opravný prostředek uplatnit osoba, jež je zaměstnancem instituce nebo orgánu EU, musí se obrátit na Soud pro veřejnou službu Evropské unie.

Příklad: Věc *Evropská komise proti Bavarian Lager Co. Ltd*[213] ukazuje dostupné opravné prostředky proti jednání nebo rozhodnutím institucí nebo orgánů EU v souvislosti s ochranou údajů.

Společnost Bavarian Lager žádala Evropskou komisi o přístup k úplnému znění zápisu ze zasedání pořádaného Komisí, které se údajně týkalo právních otázek souvisejících se společností. Komise žádosti společnosti o přístup nevyhověla z důvodu převažujících zájmů na ochranu údajů.[214] Společnost Bavarian Lager uplatnila článek 32 nařízení o ochraně údajů zpracovávaných institucemi EU a podala žalobu k Soudnímu dvoru; přesněji k Soudu prvního stupně (nyní Tribunál). Soud prvního stupně ve svém rozhodnutí ve věci T-194/04, *Bavarian Lager proti Komisi,* zrušil rozhodnutí Komise, jímž byla zamítnuta žádost o přístup. Evropská komise proti tomuto rozhodnutí podala opravný kasační prostředek k Soudnímu dvoru EU. Soudní dvůr (velký senát) vynesl rozsudek, v němž zrušil rozsudek Soudu prvního stupně a potvrdil rozhodnutí Evropské komise zamítnout žádost o přístup.

## 5.3.4. Sankce

**Podle práva RE** článek 10 úmluvy č. 108 stanoví, že každá smluvní strana musí stanovit vhodné postihy a opravné prostředky pro případ porušení ustanovení

213 Rozsudek Soudního dvora ze dne 29. června 2010, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd.*

214 Pro analýzu argumentu viz: EIOÚ (2011), *Veřejný přístup k dokumentům, které obsahují osobní údaje, poté, co byl vydán rozsudek ve věci Bavarian Lager,* Brusel, EIOÚ, k dispozici na adrese: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

vnitrostátního práva uplatňujícího základní zásady ochrany údajů stanovené v úmluvě č. 108.[215] **Podle práva EU** článek 24 směrnice o ochraně údajů stanoví, že členské státy „přijmou vhodná opatření, kterými zajistí uplatňování ustanovení této směrnice, a zejména určí sankce, které se uplatní v případě porušení předpisů přijatých [na základě této směrnice]".

Oba nástroje členským státům poskytují velkou volnost při rozhodování o výběru vhodných sankcí a opravných prostředků. Žádný z těchto právních nástrojů neobsahuje konkrétní pokyny ohledně povahy nebo typu vhodných sankcí ani příklady sankcí.

Avšak:

> *„although EU Member States enjoy a margin of discretion in determining what measures are most appropriate for safeguarding rights that individuals derive from EU law, in line with the principle of loyal cooperation as laid down in Article 4 (3) of the TEU, the minimum requirements of effectiveness, equivalence, proportionality and dissuasiveness should be respected"*
> *[přestože členské státy mají velkou volnost při stanovení, jaká opatření jsou nejvhodnější k ochraně práv, která pro jednotlivce vyplývají z práva EU, v souladu se zásadou loajální spolupráce stanovené v čl. 4 odst. 3 SEU musí být splněny minimální požadavky na účinnost, rovnocennost, proporcionalitu a odrazující účinek].*[216]

Soudní dvůr opakovaně uvedl, že vnitrostátní právo nemá při stanovování sankcí naprostou volnost.

Příklad: Ve věci *Von Colson a Kamann proti Land Nordrhein-Westfalen*[217] Soudní dvůr poukázal na to, že všechny členské státy, jimž je směrnice určena, jsou povinny přijmout v rámci svých vnitrostátních právních řádů všechna opatření nezbytná k zajištění plné účinnosti směrnice v souladu s cílem, který sleduje. Soudní dvůr rozhodl, že přestože členské státy mají svobodu volby způsobů a prostředků určených k zajištění provádění směrnice, tato svoboda se však

215 Rozsudek ESLP ze dne 17. července 2008, *I. proti Finsku*, č. 20511/03; rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, č. 2872/02.

216 FRA (2012), Stanovisko Agentury Evropské unie pro základní práva k navrhovanému balíčku opatření pro reformu ochrany údajů, 2/2012, Vídeň, 1. října 2012, s. 27.

217 Rozsudek Soudního dvora ze dne 10. dubna 1984, C-14/83, *Sabine von Kolson a Elisabeth Kamann proti Land Nordrhein-Westfalen*.

nedotýká povinnosti jim uložené. Zejména musí být k dispozici účinný opravný prostředek, který jednotlivci umožní sledovat a uplatňovat dotčené právo v plném věcném rozsahu. Aby byla zajištěna skutečná a účinná ochrana, musí opravné prostředky zahájit trestní řízení nebo řízení o náhradu škody, jehož výsledkem jsou sankce s odrazujícím účinkem.

Co se týče sankcí pro porušení práva EU institucemi nebo orgány EU, vzhledem ke zvláštní povaze nařízení o ochraně údajů zpracovávaných institucemi EU se počítá pouze se sankcemi ve formě disciplinárních postihů. V souladu s článkem 49 nařízení „[j]akékoli porušení povinností vyplývajících z tohoto nařízení, ať úmyslné nebo z nedbalosti, vystavuje úředníky nebo ostatní zaměstnance Evropských společenství disciplinárním postihům […]“.

# 6

# Předávání údajů do zahraničí

| EU | Probíraná témata | RE |
|---|---|---|
| **Předávání údajů do zahraničí** | | |
| Čl. 25 odst. 1 směrnice o ochraně údajů<br>Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist* | **Definice** | Čl. 2 odst. 1 dodatkového protokolu k úmluvě č. 108 |
| **Volný pohyb údajů** | | |
| Čl. 1 odst. 2 směrnice o ochraně údajů | **Mezi členskými státy EU** | |
| | **Mezi smluvními stranami úmluvy č. 108** | Čl. 12 odst. 2 úmluvy č. 108 |
| Článek 25 směrnice o ochraně údajů | **Do třetích zemí s odpovídající úrovní ochrany údajů** | Čl. 2 odst. 1 dodatkového protokolu k úmluvě č. 108 |
| Čl. 26 odst. 1 směrnice o ochraně údajů | **Do třetích zemí ve zvláštních případech** | Čl. 2 odst. 2 písm. a) dodatkového protokolu k úmluvě č. 108 |
| **Omezené předávání údajů do třetích zemí** | | |
| Čl. 26 odst. 2 směrnice o ochraně údajů<br>Čl. 26 odst. 4 směrnice o ochraně údajů | **Smluvní doložky** | Čl. 2 odst. 2 písm. b) dodatkového protokolu k úmluvě č. 108<br>Pokyny k vypracování smluvních doložek |
| Čl. 26 odst. 2 směrnice o ochraně údajů | **Závazná podniková pravidla** | |
| Příklady:<br>Dohoda mezi EU a USA o PNR<br>Dohoda mezi EU a USA o SWIFT | **Zvláštní mezinárodní dohody** | |

Směrnice o ochraně údajů stanoví nejenom volný pohyb údajů mezi členskými státy, ale obsahuje také ustanovení týkající se požadavků na předávání osobních údajů do třetích zemí mimo EU. RE rovněž uznala důležitost provedení pravidel pro předávání údajů do třetích zemí a v roce 2001 přijala dodatkový protokol k úmluvě č. 108. Tento protokol přejal hlavní regulační prvky týkající se předávání údajů do zahraničí od stran úmluvy a členských států EU.

## 6.1. Povaha předávání údajů do zahraničí

### Hlavní body

- Předáváním údajů do zahraničí se rozumí předávání osobních údajů příjemci (osobě či subjektu), který podléhá zahraniční jurisdikci.

Čl. 2 odst. 1 dodatkového protokolu k úmluvě č. 108 popisuje předávání údajů do zahraničí jako přenos údajů příjemci podléhajícímu zahraniční jurisdikci. Čl. 25 odst. 1 směrnice o ochraně údajů upravuje „předávání osobních údajů, které jsou předmětem zpracování nebo které mají být předmětem zpracování po předání, do třetích zemí […]“. Takové předávání údajů je povoleno pouze v souladu s pravidly stanovenými v článku 2 dodatkového protokolu k úmluvě č. 108 a pro členské státy EU dále v článcích 25 a 26 směrnice o ochraně údajů.

Příklad: Ve věci *Bodil Lindqvist*[218] Soudní dvůr rozhodl, že „úkon, kdy se na internetové stránce odkáže na různé osoby a tyto 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“.

Soud poté poukázal na to, že směrnice také stanoví zvláštní pravidla, jejichž účelem je umožnit členským státům dohled nad předáváním osobních údajů do třetích zemí.

Avšak vzhledem za prvé ke stavu rozvoje internetu v době vypracování směrnice a dále k tomu, tato směrnice neobsahuje kritéria platná pro používání internetu, „se nelze domnívat, že by zákonodárce Společenství měl v úmyslu

218 Rozsudek Soudního dvora ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*, body 27, 68 a 69.

výhledově zahrnout pod pojem „předávání údajů do třetí země“ i zařazení údajů na internetovou stránku […], i když jsou tyto údaje takto zpřístupněny osobám ze třetích zemí majícím technické prostředky k získání přístupu k těmto údajům.“

V opačném případě, kdyby byla směrnice „vykládán[a] v tom smyslu, že k „předání údajů do třetí země“ dochází vždy, když jsou osobní údaje uloženy na internetovou stránku, pak by toto předání bylo nutně předáním do všech třetích zemí, kde existují nezbytné technické prostředky pro přístup na internet. Zvláštní režim upravený [uvedenou směrnicí] by se tak v případě úkonů prováděných na internetu nutně stal obecně platným režimem. Jakmile by totiž Komise […] zjistila, že byť jen jediná třetí země nezajišťuje odpovídající úroveň ochrany, členské státy by byly povinny zabránit jakémukoli uvádění osobních údajů na internetu.“

Zásada, že pouhé zveřejnění (osobních) údajů nemá být považováno za předávání údajů do zahraničí, se použije také na on-line veřejné rejstříky nebo hromadné sdělovací prostředky, jako jsou (elektronické) noviny a televize. Pojmem „předávání údajů do zahraničí“ lze označit pouze komunikaci, která je určena konkrétním příjemcům.

## 6.2. Volný pohyb údajů mezi členskými státy nebo mezi smluvními stranami

### Hlavní body

- Předávání osobních údajů do jiného členského státu Evropského hospodářského prostoru nebo do jiné smluvní strany úmluvy č.108 musí být neomezené.

V souladu s čl. 12 odst. 2 úmluvy č. 108, **podle práva RE** musí existovat volný pohyb osobních údajů mezi stranami úmluvy. Vnitrostátní právo nesmí omezovat předávání údajů na území jiné smluvní strany, pokud:

- to nevyžaduje zvláštní povaha údajů,[219]

219 Čl. 12 odst. 3 písm. a) úmluvy č. 108.

- omezení je nezbytné, aby se zamezilo obcházení vnitrostátních právních ustanovení o předávání údajů třetím osobám.[220]

**Podle práva EU** omezování nebo zakazování volného pohybu údajů mezi členskými státy z důvodů ochrany údajů zakazuje čl. 1 odst. 2 směrnice o ochraně údajů. Oblast volného pohybu údajů byla rozšířena Dohodou o Evropském hospodářském prostoru (EHP),[221] kterou se vnitřní trh rozšiřuje o Island, Lichtenštejnsko a Norsko.

Příklad: Jestliže přidružená společnost mezinárodní skupiny společností usazené v několika členských státech, mezi nimi ve Slovinsku a Francii, předává osobní údaje ze Slovinska do Francie, takový pohyb údajů nesmí být omezený nebo zakázaní vnitrostátním právem Slovinska.

Jestliže však tatáž slovinská přidružená společnost chce stejné údaje předávat do mateřské společnosti ve Spojených státech, musí slovinský vývozce údajů dodržovat postup stanovený ve slovinském právu pro předávání údajů do třetích zemí, jež nemají odpovídající ochranu údajů, pokud mateřská společnost neschválila zásady „bezpečného přístavu", dobrovolný kodex chování o zajištění odpovídající úrovně ochrany údajů (viz oddíl 6.3.1).

Předávání údajů do členských států EHP pro účely, které nespadají do působnosti vnitřního trhu, jako je například vyšetřování trestných činů, však není předmětem ustanovení směrnice o ochraně údajů, a tudíž se na ně nevztahuje zásada volného pohybu údajů. Co se týče práva RE, všechny oblasti spadají do působnosti úmluvy č. 108 a dodatkového protokolu k úmluvě č. 108, přestože smluvní strany mohou stanovit výjimky. Všichni členové EHP jsou též stranami úmluvy č. 108.

220 *Tamtéž,* čl. 12 odst. 3 písm. b).

221 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.

# 6.3. Volný pohyb údajů do třetích zemí

## Hlavní body

- Předávání osobních údajů do třetích zemí nesmí být omezováno vnitrostátními právními předpisy o ochraně údajů, jestliže:
  - byla zjištěna přiměřenost ochrany údajů na straně příjemce nebo
  - je to nezbytné vzhledem ke zvláštním zájmům subjektu údajů nebo legitimním převládajícím zájmům druhých, zejména důležitých veřejných zájmů.
- Přiměřeností ochrany údajů třetí země se rozumí, že do vnitrostátního práva této země byly účinným způsobem provedeny hlavní zásady ochrany údajů.
- Podle práva EU přiměřenost ochrany údajů v třetí zemi posuzuje Evropská komise. Podle práva RE je úprava způsobu posuzování přiměřenosti ponechána na vnitrostátním právu.

## 6.3.1. Volný pohyb údajů díky odpovídající ochraně

**Právo RE** povoluje, aby vnitrostátní právní předpisy umožnily volný pohyb údajů do států, jež nejsou smluvními stranami, jestliže stát příjemce nebo organizace pro zamýšlené předávání údajů zajišťuje odpovídající úroveň ochrany.[222] Vnitrostátní právo rozhoduje o způsobu posuzování úrovně ochrany v cizí zemi i o tom, kdo by posouzení měl provádět.

**Podle práva EU** volný pohyb údajů do třetích zemí s odpovídající úrovní ochrany údajů stanoví čl. 25 odst. 1 směrnice o ochraně údajů. Díky požadavku přiměřenosti spíše než rovnocennosti je možné uznávat různé způsoby provádění ochrany údajů. V souladu s čl. 25 odst. 6 směrnice je Evropská komise kompetentní k posuzování úrovně ochrany údajů v cizích zemích prostřednictvím rozhodnutí o přiměřenosti a při tom konzultuje s pracovní skupinou zřízenou podle článku 29, která významným způsobem přispěla k výkladu článků 25 a 26.[223]

222 Čl. 2 odst. 1 dodatkového protokolu k úmluvě č. 108.

223 Viz např. pracovní skupina zřízená podle článku 29 (2003), Pracovní dokument o předávání osobních údajů do třetích zemí: Uplatňování čl. 26 odst. 2 směrnice EU o ochraně údajů na závazná podniková pravidla pro mezinárodní předávání údajů, WP 74, Brusel, 3. června 2003, a 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.

Rozhodnutí Evropské komise o přiměřenosti je závazné. Jestliže Evropská komise zveřejní rozhodnutí o přiměřenosti pro určitou zemi v *Úředním věstníku Evropské unie*, jsou všechny členské země EHP a jejich orgány zavázány se tímto rozhodnutím řídit, což znamená, že do této země lze předávat údaje bez nutnosti provádění kontrol nebo licenčních řízení před vnitrostátními orgány.[224]

Evropská komise může též hodnotit části právního systému země nebo se omezit na jednotlivá témata. Komise například vydala rozhodnutí o přiměřenosti výlučně v souvislosti s obchodními právními předpisy Kanady pro soukromý sektor.[225] Existuje též několik rozhodnutí o přiměřenosti týkajících se předávání údajů na základě dohod mezi EU a cizími státy. Tato rozhodnutí se týkají výlučně jednoho typu předávání údajů, jako je předávání údajů jmenné evidence cestujících leteckými společnostmi zahraničním orgánům hraniční kontroly, když letecká společnost létá z EU do některých zámořských destinací (viz oddíl 6.4.3). V souladu s novější praxí v oblasti předávání údajů vycházející ze zvláštních smluv mezi EU a třetími zeměmi se obecně ruší nutnost rozhodnutí o přiměřenosti, jelikož se má za to, že dohoda sama poskytuje odpovídající úroveň ochrany údajů.[226]

Jedno z nejdůležitějších rozhodnutí o přiměřenosti se ve skutečnosti netýká souboru právních ustanovení.[227] Týká se spíše pravidel, svou povahou připomínajících kodex chování, známých jako zásady „bezpečného přístavu". Tyto zásady vypracovaly EU a Spojené státy pro americké obchodní společnosti. Členem bezpečného přístavu se společnost stává dobrovolným závazkem prohlášeným před Ministerstvem obchodu Spojených států a zdokumentovaným prostřednictvím seznamu zveřejňovaným ministerstvem. Jelikož jedním z důležitých prvků přiměřenosti je účinnost provádění ochrany údajů, dohoda o bezpečném přístavu stanoví též určitou míru státního

224 Průběžně aktualizovaný seznam zemí, jimž bylo vydáno rozhodnutí o přiměřenosti, naleznete na domovské stránce generálního ředitelství pro spravedlnost Evropské komise na adrese: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

225 Evropská komise (2002), rozhodnutí 2002/2/ES 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.

226 Například Dohoda mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států (Úř. věst. 2012 L 215, s. 5–14) nebo Dohoda mezi Evropskou unií a Spojenými státy americkými o zpracovávání a předávání údajů o finančních transakcích z Evropské unie do Spojených států pro účely Programu pro sledování financování terorismu, Úř. věst 2010 L 8, s. 11–16.

227 Evropská komise (2000), 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. 2000 L 215.

dozoru: členy bezpečného přístavu se mohou stát pouze společnosti podléhající dozoru Federální obchodní komise Spojených států (Federal Trade Commission).

## 6.3.2. Volný pohyb údajů ve zvláštních případech

**Podle práva RE**, čl. 2 odst. 2 dodatkového protokolu k úmluvě č. 108 povoluje předávání osobních údajů do třetích zemí, které neposkytují odpovídající úroveň ochrany, pokud takové předávání umožňuje vnitrostátní právo a je nezbytné z důvodu:

- zvláštních zájmů subjektu údajů nebo
- oprávněných všeobecných zájmů druhých, zejména významných veřejných zájmů.

**Podle práva EU**, čl. 26 odst. 1 směrnice o ochraně údajů obsahuje ustanovení podobná ustanovením dodatkového protokolu k úmluvě č. 108.

Podle směrnice může být volný pohyb údajů do třetí země oprávněn na základě zájmů subjektu údajů, jestliže:

- jestliže subjekt údajů udělil jednoznačný souhlas s vývozem údajů nebo
- subjekt údajů uzavře – nebo hodlá uzavřít – smluvní vztah, který jasně vyžaduje, aby údaje byly předávány příjemci v zahraničí, nebo
- byla uzavřena smlouva mezi správcem údajů a třetí osobou v zájmu subjektu údajů nebo
- předávání je nezbytné pro ochranu životně důležitých zájmů subjektu údajů,
- k předání dochází z veřejného rejstříku; to je případ všeobecných zájmů, aby široká veřejnost měla přístup k informacím ve veřejných rejstřících.

Oprávněné zájmy druhých mohou ospravedlňovat volné předávání údajů do zahraničí:[228]

228 Čl. 26 odst. 1 písm. d) směrnice o ochraně údajů.

- na základě významného veřejného zájmu, kromě záležitostí národní nebo veřejné bezpečnosti, jelikož tyto nespadají do působnosti směrnice o ochraně údajů, nebo

- za účelem zjištění, výkonu nebo obrany právních nároků.

Výše uvedené případy je třeba chápat jako výjimky z pravidla, že hladké předávání údajů do jiných zemí vyžaduje odpovídající úroveň ochrany údajů v zemi příjemce. Výjimky musí být vždy vykládány restriktivně. Toto opakovaně zdůraznila pracovní skupina zřízená podle článku 29 v souvislosti s čl. 26 odst. 1 směrnice o ochraně údajů, zejména když je souhlas domnělým základem pro předávání údajů.[229] Pracovní skupina zřízená podle článku 29 dospěla k závěru, že obecná pravidla týkající se právního významu souhlasu se použijí také na čl. 26 odst. 1 směrnice. Pokud například v kontextu pracovněprávních vztahů není jasné, že souhlas, který zaměstnanci poskytli, byl poskytnut svobodně, nemůže být předávání údajů založeno na čl. 26 odst. 1 písm. a) směrnice. V takových případech se použije čl. 26 odst. 2, který vyžaduje, aby vnitrostátní orgány pro ochranu údajů udělily povolení pro předávání údajů.

## 6.4. Omezený pohyb údajů do třetích zemí

### Hlavní body

- Předtím, než jsou údaje předány do třetích zemí, které nezajišťují odpovídající úroveň ochrany údajů, může být správce povinen předložit plánované předání údajů orgánu dozoru ke kontrole.
- Správce, který chce předávat údaje do zahraničí, musí při této kontrole, doložit dvě skutečnosti:
  - že existuje právní základ pro předání údajů příjemci a
  - že jsou zavedena opatření pro zajištění odpovídající ochrany údajů u příjemce.
- Opatření pro stanovení odpovídající ochrany údajů u příjemce mohou zahrnovat:
  - smluvní ujednání mezi správcem, který údaje vyváží, a příjemcem údajů v cizí zemi nebo

229 Viz zejména 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.

  - závazná podniková pravidla, která se zpravidla použijí na předávání údajů v rámci nadnárodní skupiny společností.
- Předávání údajů zahraničním orgánům může být též upraveno zvláštní mezinárodní smlouvou.

Směrnice o ochraně údajů a dodatkový protokol k úmluvě č. 108 povolují, aby vnitrostátní právní předpisy stanovily režimy pro předávání údajů do třetích zemí, které nezajišťují odpovídající úroveň ochrany údajů, pokud správce osobních údajů zajistil odpovídající zabezpečení u příjemce a pokud to může doložit příslušnému dozorovému orgánu. Tento požadavek je výslovně uveden pouze v dodatkovém protokolu k úmluvě č. 108, avšak považuje se za standardní postup, který je také v souladu se směrnicí o ochraně údajů.

## 6.4.1. Smluvní doložky

Jak **právo RE**, tak **právo EU** zmiňují smluvní doložky mezi správcem, který údaje vyváží, a příjemcem v třetí zemi jako možný způsob zaručení dostatečné úrovně ochrany údajů u příjemce.

Na **úrovni EU** Evropská komise za asistence pracovní skupiny zřízené podle článku 29 vypracovala standardní smluvní doložky, které byly úředně uznány rozhodnutím Komise jako důkaz o odpovídající ochraně údajů.[230] Jelikož rozhodnutí Komise jsou v členských státech závazná v celém rozsahu, vnitrostátní orgány pověřené dozorem nad předáváním údajů do zahraničí musejí tyto standardní smluvní doložky ve svých postupech uznávat.[231] Pokud se tedy správce, který údaje vyváží, a příjemce v třetí zemi dohodnou a podepíší tyto doložky, mělo by to pro orgán dozoru být dostatečným důkazem toho, že jsou zavedena odpovídající ochranná opatření.

Existence standardních smluvních doložek v právním rámci EU nezakazuje správcům, aby sepsali jiné *ad hoc* smluvní doložky. Tyto by však musely zajistit stejnou úroveň ochrany jako standardní smluvní doložky. Nejdůležitější prvky standardních smluvních doložek jsou:

- doložka ve prospěch třetí strany, která umožňuje subjektům údajů vykonávat smluvní práva i přesto, že že nejsou stranou smlouvy,

230 Čl. 26 odst. 4 směrnice o ochraně údajů.

231 Čl. 288 SFEU.

- příjemce nebo dovozce údajů se dohodnou, že v případě sporu budou podléhat řízení vnitrostátního orgánu dozoru a/nebo soudů správce, který údaje vyváží.

Nyní existují dva soubory standardních doložek pro předávání údajů mezi správci, z nichž si správce, který data vyváží, může vybrat.[232] Pro předávání údajů mezi správcem a zpracovatelem existuje pouze jeden soubor standardních smluvních doložek.[233]

V kontextu **práva RE** vypracoval poradní výbor úmluvy č. 108 příručku pro přípravu smluvních doložek.[234]

### 6.4.2. Závazná podniková pravidla (Binding Corporate Rules)

Vícestranná závazná podniková pravidla (dále „ZPP“) se často týkají několika evropských orgánů pro ochranu údajů najednou.[235] Aby mohla být ZPP schválena, je třeba zaslat návrh ZPP společně se standardizovanými formuláři žádosti vedoucímu orgánu.[236] Vedoucí orgán je uveden na standardizovaném formuláři žádosti. Tento orgán poté informuje všechny orgány dozoru v členských zemích EHP, kde jsou přidružené společnosti skupiny usazeny, přestože jejich účast v procesu hodnocení ZPP je

232 Soubor I je obsažen v příloze k 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, Evropská komise (2001), Úř. věst. 2001 L 181; soubor II je obsažen v příloze k 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, Evropská komise (2004), Úř. věst. 2004 L 385.

233 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.

234 RE, poradní výbor k úmluvě č. 108 (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection* [Pokyny pro vypracování smluvních doložek upravujících ochranu údajů při předávání osobních údajů třetím osobám, jež nejsou vázány odpovídající úrovní ochrany údajů].

235 Obsah a strukturu příslušných závazných podnikových pravidel vysvětluje pracovní dokument pracovní skupiny zřízené podle článku 29 ze dne 24. června 2008, který stanoví rámec struktury závazných podnikových pravidel, WP 154, Brusel (2008), a pracovní dokument pracovní skupiny zřízené podle článku 29 ze dne 24. června 2008, který stanoví tabulku s prvky a zásadami, jež mají být v závazných podnikových pravidlech obsaženy, WP 153, Brusel (2008).

236 Pracovní skupina zřízená podle článku 29 (2007), Doporučení č. 1/2007 ke standardní žádosti o schválení závazných podnikových pravidel pro předávání osobních údajů, WP 133, Brusel, 10. ledna 2007.

dobrovolná. Ačkoliv to není závazné, všechny dotčené orgány pro ochranu údajů by měly závěr hodnocení začlenit do svých formálních postupů udělování povolení.

## 6.4.3. Zvláštní mezinárodní dohody

EU uzavřena zvláštní dohody pro dva typy předávání údajů:

### Jmenné evidence cestujících

Jmenné evidence cestujících (PNR) jsou údaje, které shromažďují letečtí dopravci během procesu rezervace a zahrnují jména, adresy, údaje kreditní karty a čísla sedadel cestujících. V souladu s právem USA jsou společnosti leteckých dopravců povinny tyto údaje zpřístupnit Ministerstvu vnitřní bezpečnosti před odletem cestujících. To platí pro lety do a ze Spojených států.

Pro zajištění odpovídající ochrany údajů PNR v souladu s ustanoveními směrnice 95/46/ES byl v roce 2004 přijat „PNR balíček"[237]. Balíček se týkal přiměřenosti zpracování údajů uplatňované Ministerstvem vnitřní bezpečnosti Spojených států.

Poté co Soudní dvůr PNR balíček zrušil[238], podepsaly EU a Spojené státy dvě samostatné dohody s dvojím účelem: za prvé poskytnout právní základ pro sdělování údajů PNR americkým orgánům a za druhé stanovit odpovídající ochranu údajů v zemi příjemce.

První dohoda o způsobu sdílení a správy údajů v zemích EU a ve Spojených státech podepsaná v roce 2012 měla několik nedostatků a tentýž rok ji nahradila jiná dohoda, aby byla zajištěna lepší právní jistota.[239] Nová dohoda obsahuje podstatná vylepšení. Omezuje a objasňuje účely, k nimž mohou být informace používány,

237 Rozhodnutí Rady 2004/496/ES ze dne 17. května 2004 o uzavření dohody mezi Evropským společenstvím a Spojenými státy americkými o zpracování a předávání údajů jmenné evidence cestujících (PNR) Úřadu pro cla a ochranu hranic ministerstva vnitřní bezpečnosti Spojených států, Úř. věst. 2004 L 183, s. 83, a rozhodnutí Komise 2004/535/ES ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cla a ochranu hranic, Úř. věst. 2004 L 235, s. 11–22.

238 Rozsudek Soudního dvora ze dne 30. května 2006 ve spojených věcech C-317/04 a C-318/04, *Evropský parlament proti Radě Evropské unie*, body 57, 58 a 59, v němž Soudní dvůr rozhodl, že jak rozhodnutí o přiměřenosti, tak dohoda týkající se zpracovávání údajů nespadají do působnosti směrnice.

239 Rozhodnutí Rady 2012/472/EU ze dne 26. dubna 2012 o uzavření Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států, Úř. věst. 2012 L 215/4. Znění dohody je připojené k tomuto rozhodnutí, Úř. věst. 2012 L 215, s. 5–14.

jako jsou závažné mezinárodní trestné činy a terorismus, a stanoví dobu, po kterou mohou být údaje uchovávány: po šesti měsících musí být údaje anonymizovány a zamaskovány. V případě, že dojde ke zneužití údajů subjektu údajů, má každý takový subjekt právo na správní a soudní nápravu v souladu s právem Spojených států. Rovněž má právo na přístup k vlastním údajům PNR a může požadovat, aby Ministerstvo vnitřní bezpečnosti provedlo opravu údajů, včetně případného výmazu, pokud jsou informace nepřesné.

Dohoda, která vstoupila v platnost dne 1. července 2012, platí sedm let, do roku 2019.

V prosinci 2011 Rada Evropské unie schválila uzavření aktualizované dohody mezi EU a Austrálií o zpracování a předávání údajů PNR.[240] Dohoda mezi EU a Austrálií o PNR představuje další krok v agendě EU, který zahrnuje globální pokyny pro jmennou evidenci cestujících,[241] vypracování systému jmenné evidence cestujících v EU[242] a sjednávání dohod s třetími zeměmi.[243]

## Údaje o finančních transakcích

Společnost Society for Worldwide Interbank Financial Telecommunication (Společnost pro celosvětovou mezibankovní finanční komunikaci, SWIFT), která sídlí v Belgii a je zpracovatelem většiny světových převodů peněz z evropských bank a měla operační středisko v USA, které zrcadlilo všechna zpracovávání údajů, byla požádána

240 Rozhodnutí Rady 2012/381/EU ze dne 13. prosince 2011 o uzavření Dohody mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání australské správě pro cla a ochranu hranic, Úř. věst. 2012 L 186/3. Znění dohody,která nahradila předchozí dohodu z roku 2008, je připojené k tomuto rozhodnutí, Úř. věst. 2012 L 186, s. 4–16.

241 Viz zejména sdělení Komise ze dne 21. září 2010 o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí, KOM(2010) 492 v konečném znění, Brusel, 21. září 2010. Viz rovněž pracovní skupina zřízená podle článku 29 (2010), Stanovisko 7/2010 ke sdělení Komise o globálním přístupu k předávání údajů jmenné evidence cestujících do třetích zemí, WP 178, Brusel, 12. listopadu 2010.

242 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 v konečném znění, Brusel, 2. února 2011. V dubnu 2011 Evropský parlament požádal agenturu FRA o předložení stanoviska k tomuto návrhu a jeho shodě s Listinou základních práv Evropské unie. Viz: FRA (2011), Stanovisko 1/2011 – Jmenná evidence cestujících, Vídeň, 14. června 2011.

243 EU jedná o nové dohodě týkající se jmenné evidence cestujících s Kanadou, která nahradí aktuálně platnou dohodu z roku 2006.

o zpřístupnění údajů Ministerstvu financí USA za účelem vyšetřování teroristických činů.[244]

Z pohledu EU neexistoval žádný dostatečný právní základ pro zpřístupnění těchto v podstatě evropských údajů, které byly ve Spojených státech přístupné jen proto, že se tam nacházelo jedno z operačních středisek pro zpracování údajů.

V roce 2010 EU a Spojené státy uzavřely zvláštní dohodu, známou jako dohoda o SWIFT, pro zajištění nezbytného právního základu a odpovídající úrovně ochrany.[245]

Na základě této dohody jsou finanční údaje uchovávané společností SWIFT dále poskytovány Ministerstvu financí Spojených států za účelem prevence, vyšetřování, odhalování nebo stíhání teroristických činů nebo financování terorismu. Ministerstvo financí Spojených států může od společnosti SWIFT požadovat finanční údaje za předpokladu, že žádost:

- co nejpřesněji identifikuje finanční údaje,
- jasně odůvodňuje nezbytnost údajů,
- je formulována tak, aby se minimalizovalo množství požadovaných údajů,
- nepožaduje žádné údaje týkající se jednotné oblasti pro platby v eurech (SEPA).

Kopie každé žádosti Ministerstva financí Spojených států musí být zaslána Europolu, který ověří, zda jsou dodržovány zásady dohody o SWIFT, či nikoli.[246] Pokud se potvrdí, že ano, musí SWIFT poskytnout finanční údaje přímo Ministerstvu financí

244 V této souvislosti viz 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; rozhodnutí belgické Komise pro ochranu soukromí (*Commission de la protection de la vie privée*) ze dne 9. prosince 2008 *„Control and recommendation procedure initiated with respect to the company SWIFT scrl"* [Postup kontroly a vydávání doporučení zahájený v souvislosti se společností SWIFT scrl] (2008).

245 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 připojené k tomuto rozhodnutí, Úř. věst. 2010 L 195, s. 5–14.

246 Společný kontrolní orgán Europolu provedl audity činností Europolu v této oblasti, jejichž výsledky jsou k dispozici na adrese: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

Spojených států. Ministerstvo musí finanční údaje uchovávat ve fyzicky zabezpečeném prostředí, kde k nim mají přístup pouze analytici vyšetřující teroristické činy nebo financování terorismu, a finanční údaje nesmějí být propojeny s žádnou jinou databází. Obecně se finanční údaje získané od společnosti SWIFT nejpozději do pěti let od jejich obdržení vymažou. Finanční údaje, které jsou relevantní pro určitá vyšetřování nebo stíhání, mohou být uchovávány po nezbytně dlouhou dobu pro tato vyšetřování nebo stíhání.

Ministerstvo financí Spojených států může informace z údajů, jež obdrželo od společnosti SWIFT, předávat konkrétním donucovacím orgánům, orgánům veřejné bezpečnosti nebo orgánům pro boj proti terorismu v rámci nebo mimo Spojené státy výlučně pro účely vyšetřování, odhalování, prevenci nebo stíhání teroristických činů a jejich financování. Pokud se další předání finančních údajů týká občana nebo rezidenta členského státu EU, je jakékoli sdílení údajů s orgány třetí země předmětem předchozího souhlasu příslušných orgánů dotčeného členského státu. Výjimky jsou možné v případech, kdy je sdílení údajů zásadní pro prevenci bezprostředního závažného ohrožení veřejné bezpečnosti.

Na dodržování zásad dohody o SWIFT dohlížejí nezávislé orgány dozoru včetně osoby jmenované Evropskou komisí.

Subjekty údajů mají právo od příslušného orgánu pro ochranu údajů v EU obdržet potvrzení, že jejich práva na ochranu osobních údajů byla dodržena. Subjekty údajů mají též právo na opravu, výmaz nebo blokování svých údajů shromážděných a uchovávaných Ministerstvem financí Spojených států v souladu s dohodou o SWIFT. Práva subjektů údajů na přístup však mohou podléhat určitým právním omezením. Pokud je přístup zamítnut, musí být subjekt údajů písemně vyrozuměn o zamítnutí a jeho právu na správní a soudní nápravu ve Spojených státech.

Dohoda o SWIFT platí pět let, do srpna 2015. Pokud jedna ze stran neoznámí druhé straně alespoň šest měsíců předem svůj záměr dohodu neprodloužit, dohoda se automaticky prodlužuje o další období jednoho roku.

# 7

# Ochrana údajů v sektoru policie a trestního soudnictví

| EU | Probíraná témata | RE |
|---|---|---|
| | Obecně | Úmluva č. 108 |
| | Policie | Doporučení o policii |
| | | Rozsudek ESLP ze dne 17. prosince 2009, *B.B. proti Francii*, č. 5335/06 |
| | | Rozsudek ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04 |
| | | Rozsudek ESLP ze dne 31. května 2005, *Vetter proti Francii*, č. 59842/00 |
| | Kyberkriminalita | Úmluva o kyberkriminalitě |
| **Ochrana údajů v kontextu přeshraniční spolupráce policejních a justičních orgánů** | | |
| Rámcové rozhodnutí o ochraně údajů | Obecně | Úmluva č. 108 |
| | | Doporučení o policii |
| Prümské rozhodnutí | Pro zvláštní údaje: otisky prstů, DNA, výtržnictví atd. | Úmluva č. 108 |
| | | Doporučení o policii |
| Rozhodnutí o Europolu | Podle zvláštních agentur | Úmluva č. 108 |
| Rozhodnutí o Eurojustu | | Doporučení o policii |
| Nařízení o agentuře Frontex | | |
| Rozhodnutí SIS II | Podle zvláštních společných informačních systémů | Úmluva č. 108 |
| Nařízení o VIS | | Doporučení o policii |
| Nařízení o Eurodacu | | Rozhodnutí ESLP ze dne 2. února 2010, *Dalea proti Francii*, č. 964/07 |
| Rozhodnutí o CIS | | |

S cílem vyvážit zájmy jednotlivce v oblasti ochrany údajů se zájmy společnosti v oblasti shromažďování údajů za účelem boje proti kriminalitě a zajištění národní a veřejné bezpečnosti RE a EU vydaly zvláštní právní nástroje.

## 7.1. Právo RE o ochraně údajů v z sektoru policie a trestního soudnictví

**Hlavní body**

- Úmluva č. 108 a doporučení RE o policii zahrnují ochranu údajů ve všech oblastech práce policie.
- Úmluva o kyberkriminalitě (Budapešťská úmluva) je závazný mezinárodní právní nástroj, který se zabývá trestnými činy páchanými na elektronických sítích a jejich prostřednictvím.

Na úrovni EU úmluva č. 108 zahrnuje všechny oblasti zpracování údajů a její ustanovení mají upravovat zpracování osobních údajů obecně. Úmluva č. 108 se tudíž použije na ochranu údajů v oblasti práce policie a trestního soudnictví, přestože smluvní strany mohou její použití omezit.

Zákonné úkoly policie a orgánů činných v trestním řízení často vyžadují zpracování osobních údajů, které může mít pro dotčené osoby závažné důsledky. Doporučení o používání osobních údajů v policejní oblasti, které RE přijala v roce 1987, poskytuje smluvním stranám pokyny ohledně toho, jak by měly uplatňovat zásady úmluvy č. 108 v kontextu zpracování osobních údajů policejními orgány.[247]

### 7.1.1. Doporučení o policii

ESLP trvale zastává názor, že archivace a uchování osobních údajů policií nebo orgány národní bezpečnosti představuje zásah do práv zakotvených v čl. 8 odst. 1 EÚLP. Mnoho rozsudků ESLP se zabývá odůvodněním takových zásahů.[248]

247 RE, Výbor ministrů (1987), Doporučení č. Rec(87)15 členským státům, kterým se upravuje používání osobních údajů v policejní oblasti, 17. září 1987.

248 Viz např. rozsudek ESLP ze dne 26. března 1987, *Leander proti Švédsku,* č. 9248/81; rozsudek ESLP ze dne 13. listopadu 2012, *M.M. proti Spojenému království,* č. 24029/07; rozsudek ESLP ze dne 18. dubna 2013, *M.K. proti Francii*, č. 19522/09.

Příklad: Ve věci *B.B. proti Francii*[249] ESLP rozhodl, že zařazení odsouzeného sexuálního delikventa do národní soudní databáze spadá do působnosti článku 8 EÚLP. Avšak vzhledem k tomu, že byla uplatněna dostatečné ochranná opatření pro ochranu údajů, jako právo subjektu údajů požadovat výmaz údajů, omezená doba uchování údajů a omezený přístup k takovým údajům, byla zajištěna korektní rovnováha mezi soukromými a veřejnými zájmy. Soud dospěl k závěru, že nedošlo k porušení článku 8 EÚLP.

Příklad: Ve věci *S. a Marper proti Spojenému království*[250] byli oba stěžovatelé obviněni z trestných činů, avšak nikoli odsouzeni. Přesto byly jejich otisky prstů, profily DNA a buněčné vzorky uchovávány na policii. Neomezené uchovávání biometrických údajů povoloval status, kdy byla osoba podezřelá z trestného činu, i pokud byl podezřelý později zproštěn viny nebo propuštěn. ESLP rozhodl, že všeobecné a nerozlišující uchovávání osobních údajů, které není časově omezené a u něhož mají osoby zproštěné viny pouze omezené možnosti požadovat výmaz, představuje nepřiměřený zásah do práv stěžovatelů na respektování soukromého života. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Mnoho dalších rozsudků ESLP se zabývá odůvodněním zásahu do práva na ochranu údajů sledováním.

Příklad: Ve věci *Allan proti Spojenému království*[251] orgány tajně nahrávaly soukromé rozhovory vězně s přítelem v návštěvních prostorách věznice a se spoluvězněm v cele. ESLP rozhodl, že používání zařízení pro záznam zvuku a obrazu v cele stěžovatele, v návštěvních prostorách věznice a na spoluvězně představuje zásah do práva stěžovatele na soukromý život. Jelikož v dané době neexistoval žádný zákonný režim, který by upravoval používání skrytých nahrávacích zařízení policií, nebyl uvedený zásah v souladu se zákonem. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Příklad: Ve věci *Klass a další proti Německu*[252] stěžovatelé tvrdili, že několik německých legislativních aktů, jež povolují sledování e-mailu, pošty a telekomunikací, porušují článek 8 EÚLP, zejména z toho důvodu, že dotčená osoba

249 Rozsudek ESLP ze dne 17. prosince 2009, *B.B. proti Francii,* č. 5335/06.

250 Rozsudek ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, body 119 a 125.

251 Rozsudek ESLP ze dne 5. listopadu 2002, *Allan proti Spojenému království*, č. 48539/99.

252 Rozsudek ESLP ze dne 6. září 1978, *Klass a další proti Německu,* č. 5029/71.

nebyla o sledování informována a nemohla se obrátit na soudy po ukončení takového sledování. ESLP rozhodl, že hrozba sledování nutně zasahuje do svobody komunikace mezi uživateli poštovních a telekomunikačních služeb. Shledal však, že byla zavedena dostatečná ochranná opatření proti zneužití. Německá legislativa oprávněně považovala taková opatření za nezbytná v demokratické společnosti v zájmu národní bezpečnosti a pro prevenci nepokojů nebo kriminality. Soud dospěl k závěru, že nedošlo k porušení článku 8 EÚLP.

Jelikož zpracování údajů policejními orgány může mít na dotčené osoby značný dopad, jsou obzvláště důležitá podrobná pravidla o ochraně údajů pro vedení databází v této oblasti. Doporučení RE o policii usilovalo o řešení tohoto problému prostřednictvím stanovení pokynů o tom, jak by měly být údaje pro práci policie shromažďovány, jak by měly být uchovávány údaje ve spisech v této oblasti, kdo by měl mít povolen přístup k těmto spisům, včetně podmínek předávání údajů cizím policejním orgánům, jak by subjekty údajů měly být schopny vykonávat svá práva na ochranu údajů a jak by měla být prováděna kontrola nezávislými orgány. Povinnost zajistit odpovídající zabezpečení údajů je také zohledněna.

Doporučení nestanoví otevřené, neomezené shromažďování údajů policejními orgány. Omezuje shromažďování osobních údajů policejními orgány na údaje, které jsou nezbytné pro prevenci skutečného nebezpečí nebo potlačení určitého trestného činu. Jakékoli další shromažďování údajů by muselo být založeno na zvláštních vnitrostátních právních předpisech. Zpracování citlivých údajů by mělo být omezeno na takové, které je absolutně nezbytné v souvislosti s konkrétním vyšetřováním.

Jsou-li údaje shromažďovány bez vědomí subjektu údajů, měl by být subjekt údajů informován o shromažďování údajů, jakmile toto sdělení nenaruší vyšetřování. Shromažďování údajů pomocí sledování za použití techniky nebo jiných automatických prostředků by také mělo být zakotveno ve zvláštních právních ustanoveních.

Příklad: Ve věci *Vetter proti Francii*[253] anonymní svědci obvinili stěžovatele z vraždy. Jelikož stěžovatel pravidelně docházel do domu přítele, policie tam nainstalovala odposlouchávací zařízení na základě povolení vyšetřujícího soudce. Na základě zaznamenaných rozhovorů byl stěžovatel zatčen a stíhán pro trestný čin vraždy. Požádal o to, aby záznam byl prohlášen za nepřijatelný důkaz, přičemž zejména namítal, že to není stanoveno zákonem. ESLP měl rozhodnout o tom, zda je používání odposlouchávacích zařízení „v souladu se

253 Rozsudek ESLP ze dne 31. května 2005, *Vetter proti Francii*, č. 59842/00.

zákonem“, či nikoli. Instalace štěnic v soukromých prostorách zjevně nespadalo do působnosti článků 100 a násl. trestního řádu, jelikož tato ustanovení se týkala odposlouchávání telefonních linek. Článek 81 trestního řádu dostatečně jasně nestanovil rozsah nebo způsob výkonu rozhodnutí orgánů povolit sledování soukromých rozhovorů. To znamená, že stěžovateli nebyla poskytnuta minimální úroveň ochrany, na niž mají občasné v demokratické společnosti podle práva nárok. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

Rada ve svém doporučení dospěla k závěru, že při uchovávání osobních údajů je nezbytné jasně rozlišovat mezi: administrativními údaji a policejními údaji, různými typy subjektů údajů, jako jsou podezřelé osoby, odsouzené osoby, oběti a svědci, a údaji považovanými za spolehlivá fakta a údaji založenými na podezření nebo spekulaci.

Policejní údaje by měly být přísně omezeny, co se týče účelu. To má dopad na sdělování policejních údajů třetím osobám: předávání nebo sdělování takových údajů v rámci policejního sektoru by se mělo řídit tím, zda existuje oprávněný zájem na sdílení informací nebo ne. Předávání nebo sdělování takových údajů mimo policejní sektor by mělo být povoleno pouze tehdy, existuje-li jasná zákonná povinnost nebo povolení. Mezinárodní předávání nebo komunikace by měly být omezeny na cizí policejní orgány a založeny na zvláštních právních ustanoveních, případně na mezinárodních smlouvách, pokud to je nezbytné pro zamezení závažnému a bezprostřednímu nebezpečí.

Zpracování údajů policií musí být předmětem nezávislého dozoru, aby bylo zajištěno dodržování vnitrostátních právních předpisů o ochraně údajů. Subjekty údajů musí mít všechna práva na přístup zakotvená v úmluvě č. 108. Jsou-li práva subjektů údajů na přístup omezena v souladu s článkem 9 úmluvy č. 108 v zájmu účinných policejních vyšetřování, musí mít subjekt údajů podle vnitrostátního práva právo odvolat se k vnitrostátnímu orgánu dozoru pro ochranu údajů nebo k jinému nezávislému orgánu.

## 7.1.2. Budapešťská úmluva o kyberkriminalitě

Vzhledem k tomu, že se při trestné činnosti stále více používají elektronické systémy na zpracování údajů a že trestná činnost tyto systémy stále více ovlivňuje, jsou zapotřebí nové právní předpisy týkající se trestné činnosti, které tento problém budou řešit. RE tudíž přijala mezinárodní právní nástroj, Úmluvu o kyberkriminalitě – též známou jako Budapešťská úmluva – s cílem řešit otázku trestných činů páchaný

na elektronických sítích nebo jejich prostřednictvím.[254] Úmluva je otevřená k přistoupení též nečlenským státům RE a do poloviny roku 2013 byly stranou úmluvy čtyři státy, které nejsou členy RE – Austrálie, Dominikánská republika, Japonsko a Spojené státy – a dalších 12 nečlenských států ji podepsalo nebo bylo vyzváno k přistoupení.

Úmluva o kyberkriminalitě zůstává nejvlivnější mezinárodní smlouvou, která se zabývá porušováním právních předpisů prostřednictvím internetu nebo jiných informačních sítí. Vyžaduje, aby strany aktualizovaly a harmonizovaly své trestní právo proti hackerství a dalšímu porušování bezpečnosti, včetně porušování autorského práva, podvodů v oblasti informatiky, dětské pornografie a dalších ilegálních počítačových aktivit. Úmluva rovněž stanoví procesní pravomoci týkající se prohledávání počítačových sítí a odposlouchávání komunikací v souvislosti s potíráním kyberkriminality. A konečně umožňuje účinnou mezinárodní spolupráci. Dodatkový protokol k úmluvě se zabývá kriminalizací rasistické a xenofobní propagandy v počítačových sítích.

Přestože úmluvě ve skutečnosti není nástrojem pro podporu ochrany údajů, kriminalizuje činnosti, jež budou patrně porušovat právo subjektu údajů na ochranu jeho údajů. Zároveň ukládá smluvních stranám povinnost při provádění úmluvy zajistit odpovídající ochranu lidských práv a svobod, včetně práv zakotvených v EÚLP, jako je právo na ochranu údajů.[255]

## 7.2. Právo EU o ochraně údajů v sektoru policie a trestního soudnictví

### Hlavní body

- Na úrovni EU je ochrana údajů v sektoru policie a trestního soudnictví upravována pouze v souvislosti přeshraniční spolupráce policejních a justičních orgánů.
- Existují zvláštní režimy pro ochranu údajů pro Evropský policejní úřad (Europol) a Evropskou jednotku pro soudní spolupráci (Eurojust), což jsou orgány EU, jež napomáhají při přeshraničním prosazování práva a podporují je.

254 Rada Evropy, Výbor ministrů (2001), Úmluva o kyberkriminalitě ze dne 23. listopadu 2001, která vstoupila v platnost dne 1. července 2004, č. CETS 185, Budapešť.

255 *Tamtéž,* čl. 15 odst. 1.

- Zvláštní režimy pro ochranu údajů existují také pro společné informační systémy zřízené na úrovni EU pro přeshraniční výměnu informací mezi příslušnými policejními a justičními orgány. Významnými příklady jsou Schengen II, Vízový informační systém (VIS) a Eurodac, centralizovaný systém obsahující údaje o otiscích prstů občanů třetích zemí žádajících o azyl v členských státech EU.

Směrnice o ochraně údajů se nepoužije na oblast policie a trestního soudnictví. Nejvýznamnější nástroje v této oblasti popisuje oddíl 7.2.1.

## 7.2.1. Rámcové rozhodnutí o ochraně údajů

Rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech (*rámcové rozhodnutí o ochraně údajů*)[256] usiluje o zajištění ochrany osobních údajů fyzických osob při zpracovávání jejich osobních údajů za účelem předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo za účelem výkonu trestů. Jménem členských států nebo EU jednají příslušné orgány činné v oblasti policie a trestního soudnictví. Tyto orgány jsou agentury nebo orgány EU i orgány členských států.[257] Rámcové rozhodnutí se použije pouze na zajišťování ochrany údajů v rámci přeshraniční spolupráce mezi těmito orgány a nevztahuje se na národní bezpečnost.

Rámcové rozhodnutí o ochraně údajů do velké míry vychází ze zásad a definic stanovených v úmluvě č. 108 a směrnici o ochraně údajů.

Údaje musí být používány pouze příslušným orgánem a pouze za účelem, za nímž byly předány nebo zpřístupněny. Přijímající členský stát musí respektovat jakákoli omezení týkající se výměny údajů, jež stanoví právní předpisy předávajícího členského státu. Nicméně za určitých okolností je použití údajů přijímajícím státem pro jiný účel povoleno. Příslušné orgány jsou povinny vést o předávání údajů protokoly a dokumentaci, aby bylo možné v případě stížností jasně stanovit povinnosti. Předávání údajů obdržených v rámci přeshraniční spolupráce dále třetím osobám vyžaduje souhlas členského státu, z něhož údaje pocházejí, přestože v naléhavých případech existují výjimky.

Příslušné orgány musí přijmout nezbytná bezpečnostní opatření pro ochranu osobních údajů před jakoukoli nezákonnou podobou zpracování.

256 Rada Evropské unie (2008), Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech (*rámcové rozhodnutí o ochraně údajů*), Úř. věst. 2008 L 350.

257 *Tamtéž,* čl. 2 písm. h).

Každý členský stát musí zajistit, aby byl zřízen jeden nebo více nezávislých vnitrostátních orgánů dozoru pověřených poskytováním poradenství a monitorováním používání právních předpisů přijatých v souladu s rámcovým rozhodnutím o ochraně údajů. Rovněž se zabývají stížnostmi podanými jakoukoli osobou ohledně ochrany jejích práv a svobod v souvislosti se zpracováním osobních údajů příslušnými orgány.

Subjekt údajů má nárok na to být informován o zpracování svých osobních údajů a má právo na přístup, opravu, výmaz nebo blokování údajů. Pokud je výkon těchto práv ze závažných důvodů zamítnut, musí mít subjekt údajů právo se odvolat k příslušnému vnitrostátnímu orgánu dozoru a/nebo k soudu. Jestliže někdo utrpí škodu vlivem porušení vnitrostátního právního předpisu, který provádí rámcové rozhodnutí o ochraně údajů, taková osoba má nárok na náhradu škody od správce.[258] Obecně musí mít subjekty údajů možnost žádat o soudní přezkum v případě jakéhokoli porušení jejich práv, jež jim zaručuje vnitrostátní právní předpis, kterým se provádí rámcové rozhodnutí o ochraně údajů.[259]

Evropská komise navrhla reformu, která tvoří obecné nařízení o ochraně údajů[260] a obecná směrnice o ochraně údajů.[261] Tato nová směrnice nahradí stávající rámcové rozhodnutí o ochraně údajů a uplatní obecné zásady a pravidla na policejní a justiční spolupráci v trestních věcech.

## 7.2.2. Specifičtější právní nástroje o ochraně údajů v rámci přeshraniční spolupráce policie a orgánů činných v trestním řízení

Kromě rámcového rozhodnutí o ochraně údajů výměnu informací držených členskými státy ve specifických oblastech upravuje řada právních nástrojů, jako je rámcové rozhodnutí Rady 2009/315/SVV o organizaci a obsahu výměny informací z rejstříku trestů mezi členskými státy a rozhodnutí rady o způsobech

258 *Tamtéž,* článek 19.

259 *Tamtéž,* článek 20.

260 Evropská komise (2012), *Návrh nařízení Evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů)*, KOM(2012) 11 v konečném znění, Brusel, 25. ledna 2012.

261 Evropská komise (2012), *Návrh 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 (obecná směrnice o ochraně údajů)*, KOM(2012) 10 v konečném znění, Brusel, 25. ledna 2012.

spolupráce mezi finančními zpravodajskými jednotkami členských států při výměně informací.[262]

Zejména však přeshraniční spolupráce[263] mezi příslušnými orgány stále více zahrnuje výměnu údajů týkajících se přistěhovalectví. Tato oblast práva nepatří do policejních a trestněprávních věcí, ale pro práci policejních a justičních orgánů je v mnoha ohledech relevantní. Totéž platí pro údaje o zboží dováženém do EU nebo vyváženém z EU. Zrušení kontrol na vnitřních hranicích v rámci EU zvýšilo nebezpečí podvodu, což vyžaduje, aby členské státy spolupracovaly intenzivněji, zejména posílením přeshraniční výměny informací, aby mohly účinným způsobem odhalovat a stíhat porušování celních právních předpisů členských států a EU.

## Prümské rozhodnutí

Významným příkladem institucionalizované přeshraniční spolupráce prostřednictvím výměny údajů uchovávaných jednotlivými státy je nařízení Rady 2008/615/SVV o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti (*Prümské rozhodnutí*), kterým byla v roce 2008 do práva EU začleněna Prümská smlouva.[264] Prümská smlouva byla mezinárodní smlouva o policejní spolupráci, kterou v roce 2005 podepsaly Belgie, Francie, Lucembursko, Německo, Nizozemsko, Rakousko a Španělsko.[265]

Cílem Prümského rozhodnutí je pomoci členským státům zlepšit sdílení informací za účelem prevence a potírání trestné činnosti ve třech oblastech: terorismus, přeshraniční trestná činnost a nedovolená migrace. Za tímto účelem rozhodnutí stanoví ustanovení týkající se:

---

262 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.

263 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.

264 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.

265 Úmluva 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 ilegální migraci, která je k dispozici na adrese: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

- automatizovaného přístupu k profilům DNA, otiskům prstů a některým vnitrostátním údajům o registraci vozidel,
- předávání údajů v souvislosti s významnými událostmi přeshraničního rozsahu,
- předávání informací za účelem předcházení teroristickým trestným činům
- dalších opatření pro posílení přeshraniční policejní spolupráce.

Databáze, které jsou zpřístupněny v souladu s Prümským rozhodnutím, se zcela řídí vnitrostátním právem, ale výměna údajů se navíc řídí tímto rozhodnutím a nově také rámcovým rozhodnutím o ochraně údajů. Orgány příslušné k vykonávání dozoru nad takovým předáváním údajů jsou vnitrostátní orgány dozoru pro ochranu údajů.

## 7.2.3. Ochrana údajů v Europolu a Eurojustu

### Europol

Europol, donucovací orgán EU, má ústředí v Haagu a národní jednotky v každém členském státě. Europol byl zřízen v roce 1998; jeho stávající právní status jako instituce EU je založen na rozhodnutí Rady o zřízení Evropského policejního úřadu (rozhodnutí o Europolu).[266] Cílem Europolu je pomoc při prevenci a vyšetřování organizované trestné činnosti, terorismu a dalších forem závažné trestné činnosti, jak stanoví příloha k rozhodnutí o Europolu, jimiž jsou dotčeny dva či více členských států.

Za účelem dosažení svých cílů Europol zřídil informační systém Europolu, který poskytuje členským státům databázi pro výměnu informací o trestné činnosti a dalších informací prostřednictvím jejich národních jednotek Europolu. Informační systém Europolu lze použít ke zpřístupnění údajů týkajících se: osob, které jsou podezřelé z trestného činu spadajícího do působnosti Europolu nebo byly za takový čin odsouzené, nebo osob, u nichž se má na základě konkrétních podkladů za to, že takové činy spáchají. Europol a jeho národní jednotky mohou do informačního systému Europolu přímo zadávat údaje a také v něm údaje vyhledávat. Údaje může měnit, opravovat nebo mazat pouze strana, která je do systému zadala.

266 Rada Evropské unie (2009), Rozhodnutí Rady ze dne 6. dubna 2009 o zřízení Evropského policejního úřadu (Europol), Úř. věst. 2009 L 121. Viz též návrh Komise nařízení, jímž se tedy stanoví právní základ nového Europolu, jenž navazuje na Europol, který byl zřízen rozhodnutím Rady 2009/371/SVV ze dne 6. dubna 2009 o zřízení Evropského policejního úřadu (Europol), a na akademii CEPOL zřízenou rozhodnutím Rady 2005/681/SVV ze dne 20. září 2005 o zřízení Evropské policejní akademie (EPA) a nahrazuje je, COM(2013) 173 final.

Pokud je to nezbytné pro splnění jeho úkolů, může Europol údaje o trestných činech ukládat, měnit a využívat v analytických pracovních souborech. Analytické pracovní soubory se vytvářejí za účelem shromažďování, zpracování nebo využití údajů, aby podporovaly vyšetřování konkrétních trestných činů, které provádí Europol společně s členskými státy EU.

V reakci na nový vývoj bylo 1. ledna 2013 v Europolu zřízeno Evropské centrum pro boj proti kriminalitě.[267] Centrum slouží jako informační středisko v otázkách kyberkriminality, a tak přispívá k rychlejším reakcím v případě trestných činů páchaných prostřednictvím internetu, k vývoji a používání digitálních forenzních funkcí a poskytování osvědčených postupů při vyšetřování kybernetické trestné činnosti. Centrum se zaměřuje na kybernetické trestné činy, které:

- páchají organizované skupiny s cílem vytváření vysokých nezákonných zisků, jako jsou podvody na internetu,
- působí závažnou újmu oběti, např. pohlavní vykořisťování dětí,
- poškozují kritické infrastrukturní a informační systémy v EU.

Je posílen režim ochrany údajů, kterým se řídí činnost Europolu. Článek 27 rozhodnutí o Europolu stanoví, že se použijí zásady stanovené v úmluvě č. 108 a doporučení o používání osobních údajů v policejní oblasti týkající se zpracování automatizovaných a neautomatizovaných údajů. Předávání údajů mezi Europolem a členskými státy musí též splňovat pravidla stanovená v rámcovém rozhodnutí o ochraně údajů.

K zajištění dodržování platných právních předpisů o ochraně údajů a zejména toho, aby zpracovávání osobních údajů neporušovalo práva jednotlivců, byl zřízen nezávislý společný kontrolní orgán Europolu, který přezkoumává a monitoruje činnost Europolu.[268] Každý má právo na přístup k jakýmkoli osobním údajům, které o něm Europol případně uchovává, a dále právo požadovat přezkum, opravu nebo výmaz takových údajů. Pokud není spokojen s rozhodnutím Europolu ohledně výkonu těchto práv, může se odvolat k odvolacímu výboru společného kontrolního orgánu Europolu.

267 Viz také EIOÚ (2012), Stanovisko ke sdělení Evropské komise Radě a Evropskému parlamentu o zřízení Evropského centra pro boj proti kyberkriminalitě, Brusel, 29. června 2012.

268 Článek 34 rozhodnutí o Europolu.

V případě utrpění škody v důsledku právních nebo skutkových omylů v údajích uložených nebo zpracovávaných v Europolu, může poškozený podat žalobu o náhradu škody pouze k příslušnému soudu členského státu, v němž k události, ze které vznikla škoda, došlo.[269] Pokud ke škodě došlo v důsledku toho, že Europol nedodržel své zákonné povinnosti, Europol členskému státu poskytne náhradu škody.

## Eurojust

Eurojust, který byl zřízen v roce 2002, je orgán EU, jehož ústředí sídlí v Haagu, který podporuje justiční spolupráci na vyšetřováních a stíháních závažných trestných činů týkajících se alespoň dvou členských států.[270] Eurojust je příslušný k:

- podpoře a zlepšování koordinace vyšetřování a stíhání mezi příslušnými orgány různých členských států,

- usnadňování výkonu žádostí a rozhodnutí o justiční spolupráci.

Funkce Eurojustu plní národní členové. Každý členský stát do Eurojustu jmenuje jednoho soudce nebo státního zástupce, jehož status podléhá vnitrostátnímu právu a který disponuje nezbytnými pravomocemi pro plnění úkolů potřebných k podpoře a zlepšování justiční spolupráce. Národní členové dále jednají společně jako kolegium, které plní zvláštní úkoly Eurojustu.

Eurojust může zpracovávat osobní údaje v rozsahu, v jakém je to nezbytné k plnění jeho cílů. To je však omezeno na konkrétní informace týkající se osob, které jsou podezřelé ze spáchání nebo z účasti na trestném činu spadajícím do působnosti Eurojustu nebo které byly za takový čin odsouzeny. Eurojust může též zpracovávat určité informace o svědcích nebo obětech trestných činů spadajících do jeho působnosti.[271] Ve výjimečných případech může Eurojust po omezenou dobu zpracovávat rozsáhlejší osobní údaje týkající se okolností trestného činu, pokud jsou takové údaje

269 *Tamtéž,* článek 52.

270 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/JHA 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*).

271 Čl. 15 odst. 2 konsolidovaného znění rozhodnutí Rady 2002/187/SVV ve znění rozhodnutí Rady 2003/659/SVV a rozhodnutí Rady 2009/426/SVV.

bezprostředně relevantní pro probíhající vyšetřování. V rámci své působnosti může Eurojust spolupracovat s dalšími institucemi, orgány a agenturami EU a vyměňovat si s nimi osobní údaje. Eurojust může též spolupracovat a vyměňovat si osobní údaje s třetími zeměmi a organizacemi.

V souvislosti s ochranou údajů musí Eurojust zaručit úroveň ochrany, která je minimálně rovnocenná zásadám úmluvy č. 108 ve znění pozdějších předpisů. V případě výměny údajů, musí být dodržována specifická pravidla a omezení, která jsou zakotvena buď ve smlouvě o spolupráci, nebo v pracovním ujednání v souladu s rozhodnutími Rady o Eurojustu a pravidly Eurojustu pro ochranu údajů.[272]

V Eurojustu byl zřízen nezávislý společný kontrolní orgán, jehož úkolem je dohlížet na zpracování osobních údajů v Eurojustu. Na společný kontrolní orgán se může obrátit každý, kdo není spokojen s odpovědí Eurojustu na žádost o přístup, opravu, blokování nebo výmaz osobních údajů. Pokud Eurojust zpracovává osobní údaje nezákonně, odpovídá v souladu s vnitrostátním právem členského státu, kde se nachází jeho ústředí, tedy Nizozemska, za jakoukoli škodu, která subjektu údajů vznikla.

### 7.2.4. Ochrana údajů ve společných informačních systémech na úrovni EU

Kromě výměny údajů mezi členskými státy a zřízení specializovaných orgánů EU pro potírání přeshraniční kriminality, bylo na úrovni EU zřízeno několik společných informačních systémů, které slouží jako platforma pro výměnu údajů mezi příslušnými vnitrostátními orgány a orgány EU pro stanovené účely prosazování práva, včetně právních předpisů v oblasti přistěhovalectví a v celní oblasti. Některé z těchto systémů vznikly na základě mnohostranných dohod, které byly následně nahrazeny právními nástroji a systémy EU, jako je například Schengenský informační systém, Vízový informační systém, Eurodac, Eurosur nebo celní informační systém.

Za dlouhodobé provozní řízení Schengenského informačního systému druhé generace (SIS II),[273] Vízového informačního systému (VIS) a systému Eurodac odpovídá agentura EU pro rozsáhlé informační systémy (eu-LISA) zřízená v roce 2012. Hlavním

272 Ustanovení vnitřních pravidel Eurojustu pro zpracování a ochranu osobních údajů, Úř. věst. 2005 C 68/01, 19. března 2005, s. 1.

273 Nařízení Evropského parlamentu a Rady (EU) č. 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.

úkolem agentury eu-LISA je zajišťovat účinný, bezpečný a nepřetržitý provoz informačních systémů. Rovněž odpovídá za přijímání potřebných opatření pro zajištění bezpečnosti systémů a údajů.

## Schengenský informační systém

V roce 1985 několik členských států bývalých Evropských společenství uzavřelo Dohodu mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích (*Schengenská dohoda*), jejímž cílem bylo vytvořit prostor pro volný pohyb osob nerušený hraničními kontrolami v rámci schengenského území.[274] Za účelem vyvážení ohrožení veřejné bezpečnosti, k němuž by mohlo v důsledku otevřených hranic dojít, byly posíleny hraniční kontroly na vnějších hranicích schengenského prostoru i úzká spolupráce mezi vnitrostátními policejními a justičními orgány.

V důsledku toho, že k Schengenské dohodě přistoupily další státy, byl schengenský systém nakonec včleněn do právního rámce EU Amsterodamskou smlouvou.[275] Toto rozhodnutí bylo provedeno v roce 1999. Nejnovější verze Schengenského informačního systému, tzv. SIS II, byla spuštěna dne 9. dubna 2013. Nyní slouží všem členským státům EU a Islandu, Lichtenštejnsku, Norsku a Švýcarsku.[276] Do SIS II mají též přístup Europol a Eurojust.

SIS II tvoří centrální systém (C-SIS), národní systém (N-SIS) v každém členském státě a komunikační infrastruktura mezi centrálním systémem a národními systémy. C-SIS obsahuje určité údaje o osobách a věcech, které do něj vložily členské státy. C-SIS využívají vnitrostátní orgány hraniční kontroly, policie, celní orgány, vízové a justiční orgány v celém schengenském prostoru. Každý z členských států používá národní kopii systému C-SIS, označovanou jako Národní schengenské informační systémy (N-SIS), které jsou průběžně aktualizovány, čímž se aktualizuje také C-SIS. Do systému N-SIS se nahlíží a je pořízen záznam, když:

274 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.

275 Evropská společenství (1997), Amsterodamská smlouva pozměňující Smlouvu o Evropské Unii, smlouvy o založení Evropských společenství a některé související akty, Úř. věst. 1997 C 340.

276 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 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, Rada Evropské unie (2007).

- osoba nemá právo vstoupit na schengenské území nebo zde pobývat nebo
- osoba nebo věc je hledaná justičními nebo donucovacími orgány
- nebo osoba byla nahlášena jako pohřešovaná nebo
- zboží, jako bankovky, automobily, dodávky, zbraně a průkazy totožnosti, byly nahlášeny jako odcizené nebo ztracené.

V případě záznamu musí být prostřednictvím národních schengenských informačních systémů zahájeny následné kroky.

SIS II má nové funkce, jako je možnost zadávání: biometrických údajů, jako jsou otisky prstů a fotografie ; nebo nové kategorie záznamů, jako jsou odcizené lodě, letadla, kontejnery nebo platební prostředky; a rozšířené záznamy o osobách a věcech; kopie evropských zatykačů na osoby hledané za účelem zatčení, předání nebo vydání.

Rozhodnutí Rady 2007/533/SVV o zřízení, provozování a využívání Schengenského informačního systému druhé generace (Rozhodnutí SIS II) začleňuje úmluvu č. 108: „Osobní údaje zpracovávané za použití tohoto rozhodnutí se chrání v souladu s Úmluvou Rady Evropy ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů".[277] Pokud vnitrostátní policejní orgány používají osobní údaje v rámci použití rozhodnutí SIS II, musí být do vnitrostátního práva provedena ustanovení úmluvy č. 108 i doporučení o používání osobních údajů v policejní oblasti.

Na národní systém N-SIS v každém členském státě dohlíží příslušný vnitrostátní orgán dozoru. Musí prověřovat zejména kvalitu údajů, které členský stát zadává do C-SIS prostřednictvím N-SIS. Vnitrostátní orgán dozoru musí zajistit, aby byl minimálně jednou za čtyři roky proveden audit zpracování údajů v rámci národního systému N-SIS. Vnitrostátní orgány dozoru a EIOÚ spolupracují a zajišťují koordinovaný dozor nad systémem SIS, zatímco EIOÚ odpovídá za dozor nad systémem C-SIS. V zájmu průhlednosti se jednou za dva roky zasílá Evropskému parlamentu, Radě a agentuře eu-LISA společná zpráva o činnostech.

277 Rada Evropské unie (2007), 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, článek 57.

Práva přístupu jednotlivců týkající se systému SIS II mohou být vykonávána v jakémkoli členském státě, jelikož každý systém N-SIS je přesnou kopií systému C-SIS.

Příklad: Ve věci *Dalea proti Francii*[278] stěžovateli nebylo vydáno vízum pro návštěvu Francie, jelikož francouzské orgány do Schengenského informačního systému nahlásily, že by mu měl být odepřen vstup. Stěžovatel neúspěšně žádal o přístup a opravu nebo výmaz údajů u francouzské komise pro ochranu údajů a poté u Státní rady. ESLP rozhodl, že záznam stěžovatele do Schengenského informačního systému byl v souladu se zákonem a sledoval legitimní cíl chránit národní bezpečnost. Jelikož stěžovatel neprokázal, jaká újma mu ve skutečnosti v důsledku odmítnutí vstupu do schengenského prostoru vznikla, a jelikož byla zavedena dostatečná opatření, která znemožňovala přijetí svévolných rozhodnutí, byl zásah do jeho práva na respektování soukromého života přiměřený. Stížnost stěžovatele podle článku 8 byla tudíž prohlášena za nepřípustnou.

## Vízový informační systém

Vízový informační systém (VIS), který též provozuje agentura eu-LISA, byl vytvořen za účelem podpory společné vízové politiky v EU.[279] Systém VIS umožňuje členským státům výměnu víz prostřednictvím systému, který propojuje konzuláty schengenských států nacházející se v zemích mimo EU s hraničními přechody na vnějších hranicích všech schengenských států. Systém VIS zpracovává údaje týkající se žádostí o vydání krátkodobých víz pro návštěvu nebo průjezd schengenským prostorem. Díky systému VIS mohou pohraniční orgány pomocí biometrických údajů ověřit, zda osoba, která vízum předkládá, je oprávněným držitelem víza, a identifikovat osoby, které nemají žádné doklady nebo mají padělané doklady.

V souladu s nařízením 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)* lze do systému VIS zaznamenávat pouze údaje o žadateli, jeho vízech, fotografie, daktyloskopické údaje, odkazy na předchozí žádosti

278 Rozhodnutí ESLP ze dne 2. února 2010, *Dalea proti Francii*, č. 964/07.

279 Rada Evropské unie (2004), Rozhodnutí Rady 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.

a soubory žádosti společně cestujících osob.[280] Přístup do systému VIS pro vkládání, změny nebo vymazávání údajů je omezen výhradně na vízové orgány členských států, zatímco přístup za účelem prohlížení údajů je poskytován vízovým orgánům a orgánům oprávněným k provádění kontrol na hraničních přechodech na vnějších hranicích, imigračních kontrol a azylu. Za určitých podmínek mohou o přístup k údajům v systému VIS požádat vnitrostátní příslušné policejní orgány a Europol za účelem prevence, odhalování a vyšetřování teroristických a trestných činů.[281]

## Eurodac

Název Eurodac je odvozen od daktylogramů neboli otisků prstů. Jedná se o centralizovaný systém obsahující daktyloskopické údaje státních příslušníků třetích zemí, kteří žádají o azyl v jednom z členských států EU.[282] Systém funguje od ledna 2003 a pomáhá při určování členského státu příslušného k posuzování konkrétní žádosti o azyl v souladu s nařízením Rady (ES) č. 343/2003, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států (*nařízení Dublin II*).[283] Osobní údaje v Eurodacu mohou být používány pouze za účelem usnadnění uplatňování nařízení Dublin II; jakékoli jiné použití vede k uložení sankcí.

Eurodac tvoří ústřední jednotka, kterou provozuje eu-LISA a která slouží pro ukládání a porovnávání otisků prstů, a systém pro elektronické předávání údajů mezi členskými státy a ústřední databází. Členské státy pořídí a předají do systému otisky prstů každé osoby starší 14 let, která není státním příslušníkem EU nebo je bez státní příslušnosti a která žádá o azyl na jejich území nebo která je zadržena za neoprávněné překročení jejich vnějších hranic. Členské státy mohou též pořídit a předat do

280 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, Úř. věst. 2008 L 218 (nařízení o VIS), Úř. věst. 2008 L 218.

281 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.

282 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, OJ 2002 L 62 (*nařízení o systému Eurodac*).

283 Nařízení Rady (ES) č. 343/2003 ze dne 18. února 2003, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států, Úř. věst. 2003 L 50 (*nařízení Dublin II*).

systému otisky prstů osob, které nejsou státními příslušníky EU nebo jsou bez státní příslušnosti a pobývají na jejich území bez povolení.

Daktyloskopické údaje jsou v databázi Eurodacu uchovávány pouze v pseudonymizované podobě. V případě shody je druhému členskému státu sdělen pseudonym společně s názvem prvního členského státu, který daktyloskopické údaje do systému zadal. Druhý členský stát se poté obrátí na první členský stát, protože první členský stát je podle nařízení Dublin II odpovědný za zpracování žádosti o azyl.

Osobní údaje uložené v systému Eurodac, které se týkají žadatelů o azyl, jsou uchovávány po dobu 10 let od data, kdy byly otisky prstů odebrány, pokud subjekt údajů nezíská občanství členského státu EU. V takovém případě musí být údaje okamžitě vymazány. Údaje týkající se cizích státních příslušníků zadržených pro neoprávněné překročení vnějších hranic se uchovávají po dobu dvou let. Tyto údaje musí být okamžitě vymazány, jestliže subjekt údajů získá povolení k pobytu, opustí území EU nebo získá občanství členského státu.

Systém Eurodac používají kromě všech členských států EU na základě mezinárodních dohod také Island, Norsko, Lichtenštejnsko a Švýcarsko.

## Eurosur

Evropský systém ostrahy hranic (Eurosur)[284] je určen k posílení ochrany vnějších hranic schengenského prostoru odhalování, prevencí a potíráním nelegálního přistěhovalectví a přeshraniční trestné činnosti. Slouží k posílení výměny informací a operativní spolupráce mezi vnitrostátními koordinačními středisky a agenturou Frontex, agenturou EU pověřenou rozvojem a uplatňováním nové koncepce integrované správy hranic.[285] Jeho obecné cíle jsou:

- snížit počet nelegálních přistěhovalců, jejichž vstup do EU není registrován,
- snížit počet úmrtí nelegálních přistěhovalců na základě záchrany více životů na moři,

284 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.

285 Nařízení Evropského parlamentu a Rady (EU) č. 1168/2011 ze dne 25. října 2011, kterým se mění nařízení Rady (ES) č. 2007/2004 o zřízení Evropské agentury pro řízení operativní spolupráce na vnějších hranicích členských států Evropské unie, Úř. věst. 2011 L 394, (*nařízení o agentuře Frontex*).

- celkově zvýšit vnitřní bezpečnost v EU přispíváním k prevenci přeshraniční trestné činnosti.[286]

Svoji činnost zahájil dne 2. prosince 2013 ve všech členských státech s vnějšími hranicemi a v ostatních státech bude jeho činnost zahájena od 1. prosince 2014. Nařízení se použije na ostrahu pozemních, námořních a vzdušných hranic členských států.

## Celní informační systém

Dalším důležitým společným informačním systémem zřízeným na úrovni EU je celní informační systém (CIS).[287] Při vytváření vnitřního trhu byly zrušeny všechny kontroly a formality týkající se pohybu zboží na území EU, čímž se zvýšilo riziko podvodu. Toto riziko bylo vyváženo posílením spolupráce mezi celními správami členských států. Účelem systému CIS je pomáhat členským státům při prevenci, vyšetřování a stíhání závažného porušování vnitrostátních a evropských celních a zemědělských právních předpisů.

Informace obsažené v systému CIS tvoří osobní údaje týkající se zboží, dopravních prostředků, podniků, osob, zajištěného, zabraného nebo propadlého zboží nebo hotovosti. Tyto informace mohou být používány výlučně pro účely pozorování a zpravodajství nebo provádění konkrétních kontrol nebo pro strategické nebo operativní analýzy týkající se osob podezřelých z porušení celních právních předpisů.

Do systému CIS mají přístup vnitrostátní celní, daňové, zemědělské, policejní orgány a orgány veřejného zdraví i Europol a Eurojust.

286 Viz též: Evropská komise (2008), Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Prozkoumání vytvoření Evropského systému kontroly hranic (EUROSUR), KOM(2008) 68 v konečném znění, Brusel, 13. února 2008; Evropská komise (2011), Posouzení dopadu, jež je přílohou návrhu nařízení Evropského parlamentu a Rady o zřízení Evropského systému ostrahy hranic (EUROSUR), pracovní dokument útvarů Komise, SEK(2011) 1536 v konečném znění, Brusel 12. prosince 2011, s. 18.

287 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, změněný nařízením 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, Rada Evropské unie (2009); rozhodnutí Rady 2009/917/SVV ze dne 30. listopadu 2009 o používání informačních technologií pro celní účely, Úř. věst. 2009 L 323 (*rozhodnutí o CIS*).

Zpracování osobních údajů musí splňovat zvláštní pravidla, jež stanoví nařízení č. 515/97 a Úmluva CIS,[288] i ustanovení směrnice o ochraně údajů, nařízení o ochraně údajů zpracovávaných institucemi EU, úmluvy č. 108 a doporučení o používání osobních údajů v policejní oblasti. Za dozor nad tím, že systém CIS dodržuje ustanovení nařízení (ES) č. 45/2001, odpovídá EIOÚ, který minimálně jednou ročně svolá zasedání všech vnitrostátních orgánů dozoru pro ochranu údajů příslušných z hlediska otázek dozoru týkajících se systému CIS.

288 *Tamtéž.*

# 8

# Další specifické evropské právní předpisy v oblasti ochrany údajů

| EU | Probíraná témata | RE |
|---|---|---|
| Směrnice o ochraně údajů<br>Směrnice o soukromí a elektronických komunikacích | Elektronické komunikace | Úmluva č. 108<br>Doporučení o telekomunikačních službách |
| Čl. 8 odst. 2 písm. b) směrnice o ochraně údajů | Pracovní vztahy | Úmluva č. 108<br>Doporučení o údajích zaměstnanců |
| | | Rozsudek ESLP ze dne 3. dubna 2007, *Copland proti Spojenému království*, č. 62617/00 |
| Čl. 8 odst. 3 směrnice o ochraně údajů | Zdravotnická dokumentace | Úmluva č. 108<br>Doporučení o zdravotnické dokumentaci |
| | | Rozsudek ESLP ze dne 25. února 1997, *Z. proti Finsku*, č. 22009/93 |
| Směrnice o klinických hodnoceních | Klinická hodnocení | |
| Čl. 6 odst. 1 písm. b) a e) a čl. 13 odst. 2 směrnice o ochraně údajů | Statistiky | Úmluva č. 108<br>Doporučení o statistických údajích |
| Nařízení (ES) č. 223/2009 o evropské statistice<br>Rozsudek Soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu* | Oficiální statistiky | Úmluva č. 108<br>Doporučení o statistických údajích |

| EU | Probíraná témata | RE |
|---|---|---|
| Směrnice 2004/39/ES o trzích finančních nástrojů<br>Nařízení (EU) č. 648/2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů<br>Nařízení (ES) č. 1060/2009 o ratingových agenturách<br>Směrnice 2007/64/ES o platebních službách na vnitřním trhu | Údaje ve finančnictví | Úmluva č. 108<br>Doporučení 90(19) o ochraně osobních údajů používaných při platebních a jiných souvisejících operacích<br>Rozsudek ESLP ze dne 6. prosince 2012, *Michaud proti Francii*, č. 12323/11 |

V několika případech byly na evropské úrovni přijaty zvláštní právní nástroje, které podrobněji uplatňují obecná pravidla úmluvy č. 108 nebo směrnice o ochraně údajů na specifické situace.

## 8.1. Elektronické komunikace

### Hlavní body

- Specifická pravidla o ochraně údajů v oblasti telekomunikací, zejména s ohledem na telefonní služby, jsou obsažena v nařízení RE z roku 1995.
- Zpracování osobních údajů v souvislosti s poskytováním komunikačních služeb na úrovni EU upravuje směrnice o soukromí a elektronických komunikacích.
- Zachování důvěrnosti elektronických komunikací se netýká pouze obsahu komunikace, ale také provozních údajů, jako jsou informace o tom, kdo s kým komunikoval, a lokalizačních údajů, jako odkud byly údaje sdělovány.

Komunikační sítě zvyšují možnost neoprávněného zásahu do osobní sféry uživatelů, jelikož poskytují větší technické možnosti pro odposlouchávání a sledování komunikací prováděných prostřednictvím takových sítí. Proto bylo považováno za nezbytné přijmout zvláštní předpisy pro ochranu údajů za účelem řešení konkrétních rizik, kterým čelí uživatelé komunikačních služeb.

**V roce 1995 RE vydala doporučení** o ochraně údajů v oblasti telekomunikací, zejména s ohledem na telefonní služby.[289] V souladu s tímto doporučením by měly

289 RE, Výbor ministrů (1995), Doporučení č. Rec(95)4 členským státům o ochraně osobních údajů v oblasti telekomunikačních služeb, zejména s ohledem na telefonní služby, 7. února 1995.

být účely shromažďování a zpracování osobních údajů v souvislosti s telekomunikacemi omezeny na: připojení uživatele k síti, zpřístupnění konkrétní telekomunikační služby, fakturaci, ověřování, zajišťování optimálního technického provozu a rozvoj sítě a služby.

Zvláštní pozornost byla věnována také používání komunikačních sítí pro zasílání sdělení pro účely přímého marketingu. Sdělení pro účely přímého marketingu obecně nesmějí být zasílána účastníkovi, který výslovně vyjádřil nesouhlas se zasíláním reklamních sdělení. Automatizovaná telefonní zařízení pro předávání předem nahraných reklamních sdělení mohou být používána pouze, pokud k tomu účastník poskytl výslovný souhlas. Podrobná pravidla v této oblasti stanoví vnitrostátní právo.

Co se týče **právního rámce EU,** po prvním pokusu v roce 1997 byla v roce 2002 přijata směrnice o soukromí a elektronických komunikacích a změněna v roce 2009; jejím účelem bylo doplnit a konkretizovat *ustanovení směrnice o ochraně údajů v odvětví telekomunikací*.[290] Použití směrnice o soukromí a elektronických komunikacích je omezeno na komunikační služby ve veřejných elektronických sítích.

Směrnice o soukromí a elektronických komunikacích rozlišuje tři hlavní kategorie údajů vytvářených v průběhu komunikace:

- údaje představující obsah sdělení zasílaných během komunikace; tyto údaje jsou přísně důvěrné;
- údaje nezbytné pro zahájení a vedení komunikace, takzvané provozní údaje, jako jsou informace o partnerech komunikace, čase a délce komunikace;
- provozní údaje zahrnují údaje, které se konkrétně týkají umístění komunikačního zařízení, tzv. lokalizační údaje; tyto údaje jsou zároveň údaji o poloze uživatelů komunikačních zařízení a jsou obzvláště relevantní, pokud jde o uživatele mobilních komunikačních zařízení.

290 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, 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 zpracovávání 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.

Poskytovatel služby je oprávněn používat provozní údaje pouze pro účely fakturace a pro technické poskytování služby. Se souhlasem subjektu údajů však tyto údaje mohou být sděleny jiným správcům, kteří nabízejí služby s přidanou hodnotou, např. poskytnutí informace v souvislosti s polohou uživatele o další stanici metra nebo lékárně nebo předpovědi počasí pro tuto lokalitu.

Jiný přístup k údajům o komunikacích v elektronických sítích, jako je přístup za účelem vyšetřování trestných činů, musí v souladu s článkem 15 směrnice o soukromí a elektronických komunikacích splňovat požadavky na oprávněný zásah do práva na ochranu údajů, které stanoví čl. 8 odst. 2 EÚLP a potvrzují články 8 a 52 Listiny.

Změny směrnice o soukromí a elektronických komunikacích[291] z roku 2009 zavedly:

- Omezení zasílání e-mailů pro účely přímého marketingu byla rozšířena na textové zprávy, multimediální zprávy a jiné podobné aplikace; zasílání marketingových e-mailů bez předchozího souhlasu je zakázáno. Bez takového souhlasu lze marketingové e-maily zasílat pouze stávajícím zákazníkům, pokud již dříve poskytli svoji e-mailovou adresu a proti zasílání nic nenamítají.

- Členským státům byla uložena povinnost poskytovat soudní prostředky nápravy proti porušování zákazu nevyžádaných sdělení.[292]

- Používání „cookies“, softwaru, který monitoruje a zaznamenává činnost uživatele počítače, již není možné bez souhlasu uživatele počítače. Způsob vyjádření a získání souhlasu s cílem zajistit dostatečnou ochranu by mělo podrobněji upravovat vnitrostátní právo.[293]

Dojde-li k porušení ochrany údajů v důsledku neoprávněného přístupu, ztráty nebo zničení údajů, musí být okamžitě uvědoměn příslušný orgán dozoru. Uživatelé musí

291 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.

292 Viz článek 13 pozměněné směrnice.

293 Viz *tamtéž*, článek 5; viz též pracovní skupina zřízená podle článku 29 (2012), Stanovisko 04/2012 k výjimce z požadavku na souhlas s cookies, WP 194, Brusel, 7. června 2012.

být informováni, pokud jim na základě porušení ochrany údajů může vzniknout škoda.[294]

Směrnice o uchovávání údajů[295] (prohlášena za neplatnou dne 8. dubna 2014) ukládala poskytovatelům komunikačních služeb uchovávat provozní údaje, zejména pro potřeby boje proti závažné trestné činnosti, minimálně po dobu šesti a maximálně po dobu 24 měsíců bez ohledu na to, zda poskytovatel tyto údaje stále potřeboval pro fakturační účely nebo technické poskytování služby.

Členské státy EU určí nezávislé veřejné orgány, které odpovídají za sledování bezpečnosti uchovávaných údajů.

Uchovávání telekomunikačních údajů představuje jasný zásah do práva na ochranu údajů.[296] Otázkou, zda je tento zásah oprávněný, se již zabývalo několik soudních řízení v členských státech EU.[297]

> Příklad: Ve věci *Digital Rights Ireland a Seitlinger a další*[298] Soudní dvůr konstatoval, že směrnice o uchovávání údajů je neplatná. Podle Soudního dvora „tato směrnice představuje velmi rozsáhlý a zvlášť závažný zásah do [...] základních práv [...], aniž je takový zásah přesně vymezen ustanoveními umožňujícími zaručit, že je skutečně omezen na nezbytné minimum."

Zásadní otázkou v souvislosti s elektronickými komunikacemi je zásah ze strany veřejných orgánů. Prostředky pro sledování nebo odposlouchávání komunikací, jako jsou různá odposlouchávací zařízení, jsou přípustné pouze, pokud je to stanoveno zákonem a pokud to představuje nezbytné opatření v demokratické společnosti

294 Viz rovněž pracovní skupina zřízená podle článku 29 (2011), Pracovní dokument č. 01/2011 o aktuálním rámci EU v oblasti porušení ochrany osobních údajů a doporučení pro tvorbu budoucích politik, WP 184, Brusel, 5. dubna 2011.

295 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.

296 EIOÚ (2011), 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.

297 Německo, Spolkový ústavní soud (*Bundesverfassungsgericht*), 1 BvR 256/08, 2. března 2010; Rumunsko, Federální ústavní soud (*Curtea Constituţionalã a României*), č. 1258, 8. října 2009 (*Ústavní soud České republiky*), 94/2011 Sb., 22. března 2011.

298 Rozsudek Soudního dvora ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12, *Digital Rights Ireland a Seitlinger a další*, bod 65.

v zájmu: ochrany státní bezpečnosti, veřejné bezpečnosti, finanční zájmy státu nebo potírání trestných činů nebo ochrany subjektu údajů nebo práv a svobod druhých.

Příklad: Ve věci *Malone proti Spojenému království*[299] byl stěžovatel obviněn z řady trestných činů týkajících se nepoctivého nakládání s ukradeným zbožím. Během jeho procesu vyšlo najevo, že byl na příkaz vydaný ministrem vnitra (Secretary of State for the Home Department) odposloucháván telefonický rozhovor stěžovatele. Přestože komunikace stěžovatele byla, pokud jde o vnitrostátní právo, zachycena zákonným způsobem, ESLP shledal, že neexistují žádné právní předpisy, které by upravovaly rozsah a způsob výkonu pravomoci veřejných orgánů v této oblasti, a že zásah, jež je výsledkem existence dotčené praxe, tudíž není „v souladu se zákonem". Soud rozhodl, že došlo k porušení článku 8 EÚLP.

## 8.2. Údaje zaměstnanců

### Hlavní body

- Konkrétní pravidla týkající se ochrany údajů v pracovních vztazích obsahuje doporučení RE o údajích zaměstnanců.
- Ve směrnici o ochraně údajů jsou pracovní vztahy konkrétně zmiňovány pouze v souvislosti se zpracováním citlivých údajů.
- Platnost souhlasu, který musí být svobodně poskytnut, jako právního základu pro zpracování údajů o zaměstnancích může být vzhledem k ekonomické nerovnováze mezi zaměstnavatelem a zaměstnanci sporná. Je zapotřebí pečlivě posoudit okolnosti, za nichž byl souhlas poskytnut.

V EU neexistuje žádný specifický právní rámec, který by upravoval zpracování údajů v souvislosti se zaměstnáním. Ve směrnici o ochraně údajů jsou pracovní vztahy konkrétně zmiňovány pouze v čl. 8 odst. 2, který se týká zpracování citlivých údajů. Pokud jde o RE, v roce 1989 bylo vydáno doporučení o údajích zaměstnanců, které se v současné době aktualizuje.[300]

299 Rozsudek ESLP ze dne 26. srpna 1985, *Malone proti Spojenému království*, č. 8691/79.

300 Rada Evropy, Výbor ministrů (1989), Doporučení č. Rec(89)2 členským státům o ochraně osobních údajů používaných pro pracovněprávní účely, 18. října 1989. Dále viz studie poradního výboru úmluvy č. 108 ze dne 9. září 2011 o doporučení č. R (89) 2 o ochraně osobních údajů používaných pro pracovněprávní účely a o doporučení návrhů na revizi výše uvedeného doporučení.

Průzkum nejčastějších problémů v oblasti ochrany údajů, které jsou specifické v kontextu zaměstnání, obsahuje pracovní dokument pracovní skupiny zřízené podle článku 29.[301] Pracovní skupina analyzovala význam souhlasu jako právního základu pro zpracování údajů zaměstnanců.[302] Pracovní skupina shledala, že ekonomická nerovnováha mezi zaměstnavatelem, který souhlas požaduje, a zaměstnancem, který jej poskytuje, často vzbuzuje pochyby ohledně toho, zda byl souhlas poskytnut svobodně. Proto je zapotřebí při posuzování platnosti souhlasu v kontextu zaměstnání pečlivě zvážit okolnosti, za nichž je souhlas požadován.

Častým problémem v oblasti ochrany údajů v dnešním typickém pracovním prostředí je oprávněný rozsah sledování elektronických komunikací zaměstnanců na pracovišti. Často se tvrdí, že tento problém lze snadno vyřešit zákazem soukromého používání komunikačních zařízení v práci. Takový obecný zákaz by však mohl být nepřiměřený a nerealistický. V této souvislosti je obzvláště zajímavý následující rozsudek ESLP:

Příklad: Ve věci *Copland proti Spojenému království*[303] bylo tajně sledováno používání telefonu, e-mailu a internetu zaměstnankyně univerzity s cílem ujistit se, zda z její strany nedochází k nadměrnému používání zařízení univerzity pro osobní účely. ESLP rozhodl, že telefonické hovory z prostor podniku jsou zahrnuty pod pojmem soukromý život a korespondence. Takové hovory a e-maily zasílané z práce i informace získané na základě sledování používání internetu pro osobní účely jsou tudíž chráněné článkem 8 EÚLP. V případě stěžovatelky neexistovaly žádné předpisy, které by upravovaly okolnosti, za nichž zaměstnavatelé mohou sledovat používání telefonu, e-mailu a internetu zaměstnancem. Tento zásah tudíž nebyl v souladu se zákonem. Soud dospěl k závěru, že došlo k porušení článku 8 EÚLP.

V souladu s doporučením RE o údajích zaměstnanců by měly být osobní údaje shromažďované pro účely výkonu zaměstnání od jednotlivých zaměstnanců získávány přímo.

301 Pracovní skupina zřízená podle článku 29 (2001), Stanovisko 8/2001 ke zpracování osobních údajů v pracovněprávním kontextu, WP 48, Brusel, 13. září 2001.

302 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.

303 Rozsudek ESLP ze dne 3. dubna 2007, *Copland proti Spojenému království*, č. 62617/00.

Osobní údaje získané za účelem náboru musí být omezeny na informace nezbytné pro posouzení vhodnosti uchazečů a jejich kariérního potenciálu.

Doporučení též výslovně zmiňuje kritické údaje týkající se výkonu nebo potenciálu jednotlivých zaměstnanců. Kritické údaje musí vycházet z korektního a řádného hodnocení a nesmí být formulované urážlivým způsobem. To vyžadují zásady korektního zpracování údajů a přesnosti údajů.

Specifickým aspektem práva v oblasti ochrany údajů ve vztahu mezi zaměstnavatelem a zaměstnancem je úloha zástupců zaměstnanců. Takoví zástupci mohou obdržet osobní údaje zaměstnanců pouze v takové míře, která je nezbytná k tomu, aby mohli zastupovat zájmy zaměstnanců.

Citlivé údaje shromažďované za účelem výkonu zaměstnání mohou být zpracovávány pouze v určitých případech a v souladu s ochrannými opatřeními, jež stanoví vnitrostátní právo. Zaměstnavatelé mohou žádat zaměstnance nebo uchazeče o zaměstnání, aby uvedli zdravotní stav nebo aby absolvovali lékařskou prohlídku pouze, pokud je to nezbytné pro: určení, zda jsou pro zaměstnání vhodní, pro plnění požadavků preventivní medicíny nebo aby bylo možné získat sociální dávky. Údaje o zdravotním stavu nesmí být získávány z jiných zdrojů než od dotčeného zaměstnance vyjma případů, kdy k tomu byl udělen výslovný a vědomý souhlas nebo kdy to stanoví vnitrostátní právo.

V souladu s doporučením o údajích zaměstnanců by měli být zaměstnanci informováni o účelu zpracování jejich osobních údajů, typu uchovávaných osobních údajů, subjektech, kterým jsou údaje běžně sdělovány, a o účelu a právním základu takového sdělování. Zaměstnavatelé by rovněž měli své zaměstnance předem informovat o zavedení nebo přizpůsobení automatizovaných systémů pro zpracování osobních údajů zaměstnanců nebo pro sledování pohybu nebo výkonosti zaměstnanců.

Zaměstnanci musejí mít právo na přístup ke svým údajům i na jejich opravu nebo výmaz. V případě zpracování hodnotících údajů musí mít zaměstnanci také právo na námitku proti hodnocení. Tato práva však mohou být dočasně omezena za účelem interních šetření. Je-li zaměstnanci odmítnut přístup, oprava nebo výmaz osobních údajů zaměstnanců, musí vnitrostátní právo stanovit odpovídající postupy pro na námitku proti takovému odmítnutí.

## 8.3. Zdravotnická dokumentace

### Hlavní bod

- Zdravotnická dokumentace představuje citlivé údaje, a tudíž požívá zvláštní ochrany.

Osobní údaje týkající se zdravotního stavu subjektu údajů se podle čl. 8 odst. 1 směrnice o ochraně údajů a článku 6 úmluvy č. 108 považují za citlivé údaje. Zdravotnická dokumentace tudíž podléhá přísnějšímu režimu zpracování citlivých údajů.

Příklad: Ve věci *Z. proti Finsku*[304] bývalý manžel stěžovatelky, který byl infikován virem HIV, spáchal řadu sexuálních trestných činů. Následně byl odsouzen za zabití s odůvodněním, že vědomě vystavoval své oběti riziku infekce HIV. Vnitrostátní soud nařídil, že celý rozsudek a dokumentace k věci by měly zůstat důvěrné po dobu 10 let, přestože stěžovatelka požadovala delší období zachování důvěrnosti. Odvolací soud její žádosti zamítl a v jeho rozsudku bylo uvedeno celé jméno stěžovatelky i jejího bývalého manžela. ESLP rozhodl, že takový zásah se v demokratické společnosti nepovažuje za nezbytný, protože ochrana zdravotnické dokumentace má zásadní význam pro požívání práva na respektování soukromého a rodinného života, zejména pokud jde o informace o infekci HIV vzhledem ke stigmatu, které je s tímto onemocněním v mnoha společnostech spojeno. Soud proto dospěl k závěru, že poskytnutí přístupu k informacím o totožnosti a zdravotním stavu stěžovatelky po uplynutí pouhých 10 let od vynesení rozsudku, jak bylo popsáno v rozsudku odvolacího soudu, by porušovalo článek 8 EÚLP.

Čl. 8 odst. 3 směrnice o ochraně údajů povoluje zpracování zdravotnické dokumentace, je-li to nezbytné pro účely zdravotní prevence, lékařských diagnóz, lékařské péče a ošetřování nebo správy zdravotnických služeb. Zpracování je však přípustné pouze, pokud je provádí odborný zdravotnický pracovník, který je vázán povinností zachovávat profesní tajemství, nebo jiná osoba rovněž podléhající obdobné povinnosti.[305]

304 Rozsudek ESLP ze dne 25. února 1997, *Z. proti Finsku*, č. 22009/93, body 94 a 112; viz též rozsudek ESLP ze dne 27. srpna 1997, *M. S. proti Švédsku*, č. 20837/92; rozsudek ESLP ze dne 10. října 2006, *L.L. proti Francii*, č. 7508/02; rozsudek ESLP ze dne 17. července 2008, *I. proti Finsku*, č. 20511/03; rozsudek ESLP ze dne 28. dubna 2009, *K.H. a další proti Slovensku*, č. 32881/04; rozsudek ESLP ze dne 2. června 2009, *Szuluk proti Spojenému království*, č. 36936/05.

305 Viz též rozsudek ESLP ze dne 25. listopadu 2008, *Biriuk proti Litvě*, č. 23373/03.

Doporučení RE o zdravotnické dokumentaci z roku 1997 podrobněji uplatňuje zásady úmluvy č. 108 na zpracování údajů ve zdravotnictví.[306] Navrhovaná pravidla jsou v souladu s pravidly směrnice o ochraně údajů, co se týče legitimních účelů zpracování údajů ze zdravotnické dokumentace, nezbytné podmínky, aby osoby používající údaje o zdravotním stavu, byly vázány povinností zachovávat profesní tajemství, a práv subjektů údajů na průhlednost a přístup, opravu a výmaz. Navíc zdravotnická dokumentace, kterou zákonným způsobem zpracovávají odborní zdravotničtí pracovníci, nesmí být předána donucovacím orgánům, pokud nejsou zajištěna *„sufficient safeguards to prevent disclosure inconsistent with the respect for [...] private life guaranteed under Article 8 of the ECHR"* [dostatečná ochranná opatření, která zamezí zpřístupnění údajů, které není slučitelné s respektováním [...] soukromého života v souladu s článkem 8 EÚLP].[307]

Doporučení o zdravotnické dokumentaci dále obsahuje zvláštní ustanovení týkající se zdravotnické dokumentace plodu v těle matky a nezpůsobilých osob a zpracování genetických údajů. Vědecký výzkum je výslovně uznáván jako důvod pro uchovávání údajů déle, než je potřeba, ovšem to zpravidla vyžaduje anonymizaci. Článek 12 doporučení o zdravotnické dokumentaci navrhuje podrobné předpisy pro situace, kdy výzkumníci potřebují osobní údaje a anonymizované údaje nejsou dostačující.

Vhodným prostředkem pro splnění potřeb vědeckého výzkumu může být pseudonymizace, která zároveň chrání zájmy dotčených pacientů. Pojetím pseudonymizace v souvislosti se zpracováním údajů se podrobněji zabývá oddíl 2.1.3.

Na úrovni členských států a na úrovni EU probíhá intenzivní debata o iniciativách zaměřených na uchovávání údajů o léčbě pacienta v elektronických zdravotních záznamech.[308] Zvláštním aspektem celostátních systémů elektronických zdravotních záznamů je jejich dostupnost za hranicemi: téma, jenž je v EU předmětem zvláštního zájmu v souvislosti s přeshraniční zdravotní péčí.[309]

Dalším tématem diskusí o nových předpisech jsou klinická hodnocení, jinými slovy testování nových léků na pacientech v v průběhu klinického výzkumu; toto téma

306 RE, Výbor ministrů (1997), Recommendation Rec(97)5 to member states on the protection of medical data [Doporučení č. Rec(97)5 členským státům o ochraně zdravotnické dokumentace], 13. února 1997.

307 Rozsudek ESLP ze dne 6. června 2013, *Avilkina a další proti Rusku,* č. 1585/09, bod 53 (není konečný).

308 Pracovní skupina zřízená podle článku 29 (2007), Pracovní dokument věnovaný zpracovávání osobních údajů týkajících se zdraví v elektronických zdravotních záznamech, WP 131, Brusel, 15. února 2007.

309 Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči, Úř. věst. 2011 L 88.

opět zahrnuje mnoho důsledků pro ochranu údajů. Testování léčivých přípravků humánní medicíny upravuje směrnice Evropského parlamentu a Rady 2001/20/ES ze dne 4. dubna 2001 o sbližování právních a správních předpisů členských států týkajících se uplatňování správné klinické praxe při provádění klinických hodnocení humánních léčivých přípravků (*směrnice o klinickém testování)* ).[310] V prosinci 2012 Evropská komise předložila návrh nařízení, které má směrnici o klinickém testování nahradit s cílem, aby postupy klinického hodnocení byly jednotnější a účinnější.[311]

Na úrovni EU v současné době probíhá mnoho dalších legislativních a jiných iniciativ týkajících se osobních údajů v oblasti zdravotnictví.[312]

## 8.4. Zpracování údajů pro statistické účely

### Hlavní body

- Údaje shromažďované pro statistické účely nemohou být použity k žádnému jinému účelu.
- Údaje oprávněně shromažďované za jakýmkoli účelem mohou být dále použity pro statistické účely za předpokladu, že vnitrostátní právo stanoví vhodná ochranná opatření, která uživatelé uplatňují. Za tímto účelem by měla být uplatňována zejména anonymizace nebo pseudonymizace před předáním údajů třetím osobám.

Směrnice o ochraně údajů zmiňuje zpracování údajů pro statistické účely v souvislosti s možnými výjimkami ze zásad ochrany údajů. Čl. 6 odst. 1 písm. b) směrnice stanoví, že od zásady omezení účelu se lze v souladu s vnitrostátním právem odchýlit za účelem dalšího používání údajů pro statistické účely, avšak vnitrostátní právo musí též stanovit nezbytná ochranná opatření. Čl. 13 odst. 2 směrnice povoluje stanovit omezení práv na přístup ve vnitrostátním právu, pokud jsou údaje zpracovávány výlučně pro statistické účely; zde opět musí vnitrostátní právo stanovit vhodná ochranná opatření. V této souvislosti směrnice o ochraně údajů stanoví zvláštní

310 Směrnice Evropského parlamentu a Rady 2001/20/ES ze dne 4. dubna 2001 o sbližování právních a správních předpisů členských států týkajících se uplatňování správné klinické praxe při klinickém testování léčivých přípravků humánní medicíny, Úř. věst. 2001 L 121.

311 Evropská komise (2012), *Návrh nařízení Evropského parlamentu a Rady o klinických hodnoceních humánních léčivých přípravků a o zrušení směrnice 2001/20/ES*, COM(2012) 369 final, Brusel, 17. července 2012.

312 EIOÚ (2013), Stanovisko evropského inspektora ochrany údajů ke sdělení Komise o „Akčním plánu pro elektronické zdravotnictví na období 2012–2020 – inovativní zdravotní péče pro 21. století", Brusel, 27. března 2013.

požadavek, že údaje získané nebo vytvořené během statistického výzkumu nesmějí být používány pro přijímání konkrétních rozhodnutí o subjektech údajů.

Přestože správce může údaje, které zákonným způsobem shromáždil pro jakýkoli účel, použít pro vlastní statistické účely – tzv. sekundární statistika – údaje by musely být v závislosti na kontextu anonymizovány nebo pseudonymizovány předtím, než budou předány třetí osobě pro statistické účely, pokud k tomu subjekt údajů nedal výslovný souhlas nebo pokud to výslovně nestanoví vnitrostátní právo. Vyplývá to z požadavku na vhodná ochranná opatření v souladu s čl. 6 odst. 1 písm. b) směrnice o ochraně údajů.

Nejvýznamnější případy užití údajů pro statistické účely představují oficiální statistiky, které sestavují vnitrostátní a evropské statistické úřady na základě právních předpisů členských států a EU o oficiálních statistikách. Podle těchto právních předpisů jsou občané a podniky zpravidla povinni sdělit údaje statistickým úřadům. Zaměstnanci pracující ve statistických úřadech jsou vázáni zvláštní povinností zachovávat mlčenlivost, která musí být pečlivě dodržována, jelikož je zásadní pro vysokou úroveň důvěry občanů, jež je nezbytná, pokud mají být údaje statistickým úřadům zpřístupňovány.

Nařízení (ES) č. 223/2009 o evropské statistice (*nařízení o evropské statistice*) obsahuje základní pravidla pro ochranu údajů v oficiálních statistikách, a může být proto považováno za relevantní pro předpisy týkající se oficiálních statistik na vnitrostátní úrovni.[313] Nařízení zachovává zásadu, že oficiální statistické operace vyžadují dostatečně přesný právní základ.[314]

Příklad: Ve věci *Huber proti Německu*[315] Soudní dvůr shledal, že shromažďování a uchovávání osobních údajů orgánem pro statistické účely samo o sobě nebylo dostatečným důvodem pro to, aby zpracování bylo zákonné. Právní předpis,

313 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.

314 Tato zásada má být podrobněji uvedena v kodexu Eurostatu, který v souladu s článkem 11 nařízení o evropské statistice poskytne pokyny z hlediska etiky k tomu, jak sestavovat úřední statistiky, včetně uvážlivého používání osobních údajů; k dispozici na adrese: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 Rozsudek Soudního dvora ze dne 16. prosince 2008, C-524/06, *Huber proti Německu,* viz zejména bod 68.

který stanoví zpracování osobních údajů, musí splňovat také požadavek nezbytnosti a v daném kontextu tomu tak nebylo.

Co se týče RE, doporučení o statistických údajích, které bylo vydáno v roce 1997, se zabývá vypracováváním statistik ve veřejném a soukromém sektoru.[316] Toto doporučení zavedlo zásady, které se shodují s hlavními pravidly směrnice o ochraně údajů popsanými výše. Doporučení stanoví podrobnější pravidla v těchto otázkách.

Zatímco údaje, které správce shromáždil pro statistické účely, nemohou být použity k žádnému jinému účelu, údaje, které byly shromážděny pro jiný než statistický účel, mohou být dále používány ve statistikách. Doporučení o statistických údajích dokonce povoluje sdělování údajů třetím osobám, ovšem pouze pro statistické účely. V takových případech by se strany měly písemně dohodnout na rozsahu dalšího oprávněného používání ve statistikách. Jelikož tato dohoda nemůže nahradit souhlas subjektu údajů, předpokládá se, že musejí být ve vnitrostátním právu stanovena další vhodná ochranná opatření, aby se minimalizovalo riziko zneužití osobních údajů, jako je povinnost anonymizovat nebo pseudonymizovat údaje před jejich předáním.

Zaměstnanci ve statistickém výzkumu by měli být vázáni zvláštními povinnostmi zachovávat mlčenlivost – jak je běžné pro oficiální statistiky – v souladu s vnitrostátním právem. To by mělo být rozšířeno i na tazatele, pokud jsou zapojeni do shromažďování údajů od subjektů údajů nebo jiných osob.

Pokud statistické zjišťování používající osobní údaje není stanoveno zákonem, subjekty údajů s užíváním svých údajů budou muset souhlasit, aby takové užívání bylo legitimní, nebo by měly alespoň dostat příležitost proti němu vznést námitku. Jestliže osobní údaje pro statistické účely shromažďují tazatelé, musejí být jasně informováni o tom, zda je sdělení údajů povinné v souladu s vnitrostátním právem nebo ne. Citlivé údaje by neměly být nikdy shromažďovány způsobem, který umožňuje identifikaci subjektu údajů, pokud to vysloveně nepovoluje vnitrostátní právo.

Není-li možné statistické zjišťování provést bez anonymních údajů a osobní údaje jsou opravdu nezbytné, měly by být údaje shromážděné za tímto účelem co nejdříve anonymizovány. Výsledky statistického zjišťování nesmí umožňovat identifikaci žádných subjektů údajů, pokud by to prokazatelně nepředstavovalo žádné riziko.

316 Rada Evropy, Výbor ministrů (1997), Doporučení č. Rec(97)18 členským státům o ochraně osobních údajů shromažďovaných a zpracovávaných pro statistické účely, 30. září 1997.

Po ukončení statistické analýzy by měly být osobní údaje buď vymazány, nebo anonymizovány. V tomto případě doporučení o statistických údajích navrhuje, aby identifikační údaje byly uchovávány odděleně od ostatních osobních údajů. To znamená například, že údaje by měly být pseudonymizovány a buď šifrovací klíč, nebo seznam s identifikujícími synonymy by měly být uchovávány odděleně od pseudonymizovaných údajů.

## 8.5. Údaje ve finančnictví

### Hlavní body

- Přestože údaje ve finančnictví nejsou citlivé údaje ve smyslu úmluvy č. 108 nebo směrnice o ochraně údajů, jejich zpracovávání vyžaduje určitá ochranná opatření pro zajištění přesnosti a zabezpečení údajů.
- Elektronické platební systémy musí mít zabudovanou ochranu údajů, tzv. ochranu soukromí již od návrhu (tzv. privacy by design).
- Zvláštní problémy týkající se ochrany údajů v této oblasti vznikají na základě potřeby vhodných ověřovacích mechanismů.

Příklad: Ve věci *Michaud proti Francii*[317] stěžovatel, francouzský právník, napadl svoji povinnost hlásit podezření na možné praní špinavých peněz ze strany jeho klientů, kterou mu ukládá francouzské právo. ESLP konstatoval, že požadavek, aby právníci správním orgánům hlásili informace týkající se jiné osoby, které získali na základě komunikace s danou osobou, představuje zásah do práva právníků na respektování korespondence a soukromého života v souladu s článkem 8 EÚLP, jelikož toto pojetí zahrnuje činnosti pracovní nebo obchodní povahy. Zásah však byl v souladu se zákonem a sledoval legitimní cíl, jmenovitě ochranu pořádku a předcházení trestným činům. Jelikož právníci byli povinni hlásit podezření pouze za velmi omezených okolností, ESLP rozhodl, že tato povinnost byla přiměřená, a dospěl k závěru, že nedošlo k porušení článku 8.

317 Rozsudek ESLP ze dne 6. prosince 2012, *Michaud proti Francii*, č. 12323/11; viz též rozsudek ESLP ze dne 16. prosince 1992, *Niemietz proti Německu*, č. 13710/88, bod 29, a rozsudek ESLP ze dne 25. června 1997, *Halford proti Spojenému království*, č. 20605/92, bod 42.

Použití obecného právního rámce pro ochranu údajů, jak stanoví úmluva č. 108, v kontextu plateb bylo rozpracováno v doporučení RE č. Rec(90)19 z roku 1990.[318] Toto doporučení objasňuje rozsah zákonného shromažďování a používání údajů v souvislosti s platbami, zejména prostřednictvím platebních karet. Dále vnitrostátním zákonodárcům navrhuje podrobné úpravy týkající se omezení sdělování údajů o platbách třetím osobám, časových omezení uchovávání údajů, průhlednosti, zabezpečení údajů a předávání údajů do zahraničí a nakonec také dozoru a soudního přezkumu. Navrhovaná řešení odpovídají tomu, co bylo později stanoveno jako obecný rámec EU pro ochranu údajů ve směrnici o ochraně údajů.

Je vytvářena řada právních nástrojů pro regulaci trhů finančních nástrojů a činností úvěrových institucí a investičních podniků.[319] Další právní nástroje napomáhají v boji proti obchodování zasvěcených osob a manipulaci s trhem.[320] Nejzávažnější otázky v této oblasti, které ovlivňují ochranu údajů, jsou:

- uchovávání záznamů o finančních transakcích,
- předávání osobních údajů třetím zemím,
- záznam telefonických hovorů nebo elektronických komunikací, včetně pravomoci příslušných orgánů požadovat záznamy telefonních hovorů a datových přenosů,
- sdělování osobních informací, včetně zveřejňování sankcí,

318 RE, Výbor ministrů (1990), Doporučení č. R(90)19 o ochraně osobních údajů používaných při platebních a jiných souvisejících operacích, 13. září 1990.

319 Evropská komise (2011), Návrh směrnice Evropského parlamentu a Rady o trzích finančních nástrojů a o zrušení směrnice Evropského parlamentu a Rady 2004/39/ES, KOM(2011) 656 v konečném znění, Brusel, 20. října 2011; Evropská komise (2011), Návrh nařízení Evropského parlamentu a Rady o trzích finančních nástrojů a o změně nařízení [nařízení o infrastruktuře evropských trhů] o OTC derivátech, ústředních protistranách a registrech obchodních údajů, KOM(2011) 652 v konečném znění, Brusel, 20. října 2011; Evropská komise (2011), Návrh směrnice Evropského parlamentu a Rady o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky a o změně směrnice Evropského parlamentu a Rady 2002/87/ES o doplňkovém dozoru nad úvěrovými institucemi, pojišťovnami a investičními podniky ve finančním konglomerátu, KOM(2011) 453 v konečném znění, Brusel, 20. července 2011.

320 Evropská komise (2011), Návrh nařízení Evropského parlamentu a Rady o obchodování zasvěcených osob a manipulaci s trhem (zneužívání trhu), KOM(2011) 651 v konečném znění, Brusel, 20. října 2011; Evropská komise (2011), Návrh směrnice Evropského parlamentu a Rady o trestněprávním postihu za obchodování zasvěcených osob a manipulaci s trhem, KOM(2011) 654 v konečném znění, Brusel, 20. října 2011.

- pravomoci příslušných orgánů v oblasti dozoru a provádění šetření, včetně kontrol na místě a vstupu do soukromých prostor za účelem zabavení dokumentů,
- mechanismy pro oznamování porušení, tj. programy varování, a
- spolupráce mezi příslušnými orgány členských států a Evropským orgánem pro cenné papíry a trhy (ESMA).

Existují ještě další otázky v těchto oblastech, které jsou konkrétně řešeny, včetně shromažďování údajů o finanční situaci subjektů údajů[321] nebo přeshraniční platby bankovními převody, které nevyhnutelně vedou k předávání osobních údajů.[322]

321 Nařízení Evropského parlamentu a Rady (ES) č. 1060/2009 ze dne 16. září 2009 o ratingových agenturách, Úř. věst. 2009 L 302; Evropská komise, Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (ES) č. 1060/2009 o ratingových agenturách, KOM(2010) 289 v konečném znění, Brusel, 2. června 2010.

322 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.

# 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.

EDRi, *An introduction to data protection* [Úvod do ochrany údajů], Brusel, k dispozici na adrese: www.edri.org/files/paper06_datap.pdf.

Frowein, J. a Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

Grabenwarter, C. a Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Mnichov, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. a Bates, E. (2009), *Law of the European Convention on Human Rights* [Právo Evropské úmluvy o lidských právech], Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Mnichov, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights* [Věci, materiály a komentáře k Evropské úmluvě 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 o lidských právech], 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, k dispozici na adrese: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. a Ovey, C. (2010), *The European Convention on Human Rights* [Evropská úmluva o lidských právech], Oxford, Oxford University Press.

## Kapitola 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law* [Ochrana údajů: Praktický průvodce právem Spojeného království a EU], Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paříž, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. a Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance* [Strategie ochrany údajů: Provádění dodržování ochrany údajů], Londýn, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization“ [Nedodržené sliby soukromí: Reakce na překvapivé selhání anonymizace], UCLA Law Review, roč. 57, č. 6, s. 1701–1777.

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.], k dispozici na adrese: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

## Kapitoly 3 až 5

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ v: 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.

Dammann, U. a Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agentura Evropské unie pro základní práva) (2010), *Data Protection in the European Union: the role of National Data Protection 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], Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

Úřad komisaře pro informace Spojeného království, *Privacy Impact Assessment* [Posouzení dopadu soukromí], k dispozici na adrese: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

## Kapitola 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. a Nouwt, S. (2009), *Reinventing data protection?* [Znovuobjevujeme ochranu údajů?], Berlín, Springer.

Kuner, C. (2007), *European data protection law* [Evropské právo v oblasti ochrany údajů], Oxford, Oxford University Press.

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.

## Kapitola 7

Europol (2012), *Data Protection at Europol* [Ochrana údajů v Europolu], Lucemburk, Úřad pro publikace, k dispozici na adrese: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime* [Ochrana údajů v Eurojustu: Spolehlivý, účinný a na míru vytvořený režim], Haag, Eurojust.

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.

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 dozoru 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, pracovní dokumenty CLEER 2013/2, k dispozici na adrese: www.asser.nl/upload/documents/20130226T-013310-cleer_13-2_web.pdf.

## Kapitola 8

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., 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.

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 dozoru 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.

# Judikatura

## Vybraná judikatura Evropského soudu pro lidská práva

**Přístup k osobním údajům**

*Gaskin proti Spojenému království*, č. 10454/83, 7. července 1989
*Godelli proti Itálii*, č. 33783/09, 25. září 2012
*K.H. a další proti Slovensku*, č. 32881/04, 28. dubna 2009
*Leander proti Švédsku*, č. 9248/81, 26. března 1987
*Odièvre proti Francii* [velký senát], č. 42326/98, 13. února 2003

**Vyvažování ochrany údajů se svobodou projevu**

*Axel Springer AG proti Německu* [velký senát], č. 39954/08, 7. února 2012
*Von Hannover proti Německu*, č. 59320/00, 24. června 2004
*Von Hannover proti Německu (č. 2)* [velký senát], č. 40660/08 a 60641/08, 7. února 2012

**Problémy v oblasti ochrany údajů na internetu**

*K.U. proti Finsku*, č. 2872/02, 2. prosince 2008

**Korespondence**

*Amann proti Švýcarsku* [velký senát], č. 27798/95, 16. února 2000
*Bernh Larsen Holding AS a další proti Norsku*, č. 24117/08, 14. března 2013

*Cemalettin Canli proti Turecku*, č. 22427/04, 18. listopadu 2008
*Dalea proti Francii*, č. 964/07, 2. února 2010
*Gaskin proti Spojenému království*, č. 10454/83, 7. července 1989
*Haralambie proti Rumunsku*, č. 21737/03, 27. října 2009
*Khelili proti Švýcarsku*, č. 16188/07, 18. října 2011
*Leander proti Švédsku*, č. 9248/81, 26. března 1987
*Malone proti Spojenému království*, č. 8691/79, 2. srpna 1984
*McMichael proti Spojenému království*, č. 16424/90, 24. února 1995
*M.G. proti Spojenému království*, č. 39393/98, 24. září 2002
*Rotaru proti Rumunsku* [velký senát], č. 28341/95, 4. května 2000
*S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, 4. prosince 2008
*Shimovolos proti Rusku*, č. 30194/09, 21. června 2011
*Turek proti Slovensku*, č. 57986/00, 14. února 2006

**Databáze rejstříků trestů**

*B.B. proti Francii*, č. 5335/06, 17. prosince 2009
*M.M. proti Spojenému království*, č. 24029/07, 13. listopadu 2012

**Databáze DNA**

*S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, 4. prosince 2008

**Údaje GPS**

*Uzun proti Německu*, č. 35623/05, 2. září 2010

**Údaje o zdravotním stavu**

*Biriuk proti Litvě*, č. 23373/03, 25. listopadu 2008
*I. proti Finsku*, č. 20511/03, 17. července 2008
*L.L. proti Francii*, č. 7508/02, 10. října 2006
*M.S. proti Švédsku*, č. 20837/92, 27. srpna 1997
*Szuluk proti Spojenému království*, č. 36936/05, 2. června 2009
*Z. proti Finsku*, č. 22009/93, 25. února 1997

**Totožnost**

*Ciubotaru proti Moldavsku*, č. 27138/04, 27. dubna 2010
*Godelli proti Itálii*, č. 33783/09, 25. září 2012
*Odièvre proti Francii* [velký senát], č. 42326/98, 13. února 2003

**Informace týkající se profesních činností**

*Michaud proti Francii,* č. 12323/11, 6. prosince 2012
*Niemietz proti Německu,* č. 13710/88, 16. prosince 1992

**Odposlouchávání komunikace**

*Amann proti Švýcarsku* [velký senát], č. 27798/95, 16. února 2000
*Copland proti Spojenému království*, č. 62617/00, 3. dubna 2007
*Cotlet proti Rumunsku,* č. 38565/97, 3. června 2003
*Kruslin proti Francii,* č. 11801/85, 24. dubna 1990
*Lambert proti Francii,* č. 23618/94, 24. srpna 1998
*Liberty a další proti Spojenému království*, č. 58243/00, 1. července 2008.
*Malone proti Spojenému království*, č. 8691/79, 2. srpna 1984
*Halford proti Spojenému království*, č. 20605/92, 25. června 1997
*Szuluk proti Spojenému království*, č. 36936/05, 2. června 2009

**Povinnosti zodpovědných činitelů**

*B.B. proti Francii*, č. 5335/06, 17. prosince 2009
*I. proti Finsku,* č. 20511/03, 17. července 2008
*Mosley proti Spojenému království*, č. 48009/08, 10. května 2011

**Fotografie**

*Sciacca proti Itálii,* č. 50774/99, 11. ledna 2005
*Von Hannover proti Německu,* č. 59320/00, 24. června 2004

**Právo být zapomenut**

*Segerstedt-Wiberg a další proti Švédsku,* č. 62332/00, 6. června 2006

**Právo vznést námitku**

*Leander proti Švédsku,* č. 9248/81, 26. března 1987
*Mosley proti Spojenému království*, č. 48009/08, 10. května 2011
*M.S. proti Švédsku,* č. 20837/92, 27. srpna 1997
*Rotaru proti Rumunsku* [velký senát], č. 28341/95, 4. května 2000

**Kategorie citlivých údajů**

*I. proti Finsku,* č. 20511/03, 17. července 2008

*Michaud proti Francii*, č. 12323/11, 6. prosince 2012
*S. a Marper proti Spojenému království*, č. 30562/04 a 30566/04, 4. prosince 2008

**Dohled a prosazování (úloha různých aktérů, včetně orgánů pro ochranu údajů)**

*I. proti Finsku*, č. 20511/03, 17. července 2008
*K.U. proti Finsku*, č. 2872/02, 2. prosince 2008
*Von Hannover proti Německu*, č. 59320/00, 24. června 2004
*Von Hannover proti Německu (č. 2)* [velký senát], č. 40660/08 a 60641/08, 7. února 2012

**Metody sledování**

*Allan proti Spojenému království*, č. 48539/99, 5. listopadu 2002
*Sdružení „21 Décembre 1989" a další proti Rumunsku*, č. 33810/07 a 18817/08, 24. května 2011
*Bykov proti Rusku* [velký senát], č. 4378/02, 10. března 2009
*Kennedy proti Spojenému království*, č. 26839/05, 18. května 2010
*Klass a další proti Německu*, č. 5029/71, 6. září 1978
*Rotaru proti Rumunsku* [velký senát], č. 28341/95, 4. května 2000
*Taylor-Sabori proti Spojenému království*, č. 47114/99, 22. října 2002
*Uzun proti Německu*, č. 35623/05, 2. září 2010
*Vetter proti Francii*, č. 59842/00, 31. května 2005

**Sledování pomocí kamerových systémů**

*Köpke proti Německu*, č. 420/07, 5. října 2010
*Peck proti Spojenému království*, č. 44647/98, 28. ledna 2003

**Hlasové vzorky**

*P.G. a J.H. proti Spojenému království*, č. 44787/98, 25. září 2001
*Wisse proti Francii*, č. 71611/01, 20. prosince 2005

# Vybraná judikatura Soudního dvora Evropské unie

**Judikatura týkající se směrnice o ochraně údajů**

Rozsudek ze dne 16. prosince 2008, C-73/07, *Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy a Satamedia Oy*
[Pojem „činnosti žurnalistiky“ ve smyslu článku 9 směrnice o ochraně údajů]

Rozsudek ze dne 9. listopadu 2010 ve spojených věcech C-92/09 a C-93/09, *Volker und Markus Schecke GbR a Hartmut Eifert proti Land Hessen*
[Proporcionalita zákonné povinnosti zveřejňovat osobní údaje příjemců některých zemědělských fondů EU]

Rozsudek ze dne 6. listopadu 2003, C-101/01, *Bodil Lindqvist*
[Legitimita zveřejňování údajů soukromou osobou o soukromém životě druhých na internetu]

C-131/12, *Google Spain, S.L., Google Inc. proti Agencia Española de Protección de Datos, Mario Costeja González,* žádost o rozhodnutí o předběžné otázce *Audiencia Nacional* (Španělsko) podána dne 9. března 2012, 25. května 2012, v řízení
[Povinnosti poskytovatelů vyhledávačů přestat na žádost subjektu údajů zobrazovat osobní údaje ve výsledcích vyhledávání]

Rozsudek ze dne 30. května 2013, C-270/11, *Evropská komise proti Švédskému království*
[Peněžní sankce za neprovádění směrnice]

Rozsudek ze dne 29. ledna 2008, C-275/06, *Productores de Música de España (Promusicae) proti Telefónica de España SAU*
[Povinnost poskytovatelů internetového přístupu odhalit totožnost uživatelů programu pro výměnu souborů nazvaného KaZaA sdružení pro ochranu duševního vlastnictví]

Rozsudek ze dne 8. dubna 2014, C-288/12, *Evropská komise proti Maďarsku*
[Legitimita ukončení mandátu vnitrostátního orgánu dozoru na ochranu osobních údajů]

Stanovisko generálního advokáta ze dne 13. června 2013 k věci C-291/12, *Michael Schwarz proti Stadt Bochum*

[Porušení primárního práva EU nařízením (ES) 2252/2004, které stanoví, že otisky prstů mají být uchovávány v cestovních pasech]

Rozsudek ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12, *Digital Rights Ireland a Seitling a další*

[Porušení primárního práva EU směrnicí o uchovávání údajů]

Rozsudek ze dne 16. února 2012, C-360/10, *SABAM proti Netlog N.V.*

[Povinnost poskytovatelů sociálních sítí zamezit protiprávnímu užívání hudebních a audiovizuálních děl uživateli sítí]

Rozsudek ze dne 20. května 2003, C-465/00, C-138/01 a C-139/01, *Rechnungshof proti Österreichischer Rundfunk a další a Neukomm a Lauermann proti Österreichischer Rundfunk*

[Proporcionalita zákonné povinnosti zveřejňovat osobní údaje týkající se platů zaměstnanců určitých kategorií institucí veřejného sektoru]

Rozsudek ze dne 24. listopadu 2011 ve spojených věcech C-468/10 a C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) proti Administración del Estado*

[Správné provádění čl. 7 písm. f) směrnice o ochraně údajů – „oprávněné zájmy druhých" – do vnitrostátního práva]

Rozsudek ze dne 9. března 2010, C-518/07, *Evropská komise proti Spolkové republice Německo*

[Nezávislost vnitrostátního orgánu dozoru]

Rozsudek ze dne 16. prosince 2008, C-524/06, *Huber proti Bundesrepublik Deutschland*

[Legitimita uchovávání údajů o cizincích ve statistickém rejstříku]

Rozsudek ze dne 5. května 2011, C-543/09, *Deutsche Telekom AG proti Bundesrepublik Deutschland*

[Nutnost obnoveného souhlasu]

Rozsudek ze dne 7. května 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam proti M. E. E. Rijkeboer*
[Právo přístupu subjektu údajů]

Rozsudek ze dne 16. října 2012, C-614/10, *Evropská komise proti Rakouské republice*
[Nezávislost vnitrostátního orgánu dozoru]

**Judikatura týkající se nařízení o ochraně údajů zpracovávaných institucemi EU**

Rozsudek ze dne 29. června 2010, C-28/08 P, *Evropská komise proti The Bavarian Lager Co. Ltd*
[Přístup k dokumentům]

Rozsudek ze dne 6. března 2003, C-41/00 P, *Interporc Im- und Export GmbH proti Komisi Evropských společenství*
[Přístup k dokumentům]

Rozsudek ze dne 15. června 2010, F-35/08, *Dimitrios Pachtitis proti Evropské komisi*
[Používání osobních údajů v kontextu zaměstnanosti v orgánech EU]

Rozsudek ze dne 5. července 2011, F-46/09, *V proti Parlamentu*
[Používání osobních údajů v kontextu zaměstnanosti v orgánech EU]

# Seznam

**Judikatura Soudního dvora Evropské unie**

**Judikatura Evropského soudu pro lidská práva**

**Judikatura vnitrostátních soudů**

Agentura Evropské unie pro základní práva
Evropský soud pro lidská práva - Rada Evropy

**Příručka evropského práva v oblasti ochrany údajů**

2015 — 194 s. — 14,8 × 21 cm

ISBN 978-92-871-9933-1 (Rada Evropy)
ISBN 978-92-9239-326-7 (FRA)
doi:10.2811/53430

Mnoho doplňujících informací o Agentuře Evropské unie pro základní práva (FRA) je k dispozici na internetu. Můžete se s nimi seznámit internetových stránkách agentury FRA (http://fra.europa.eu).

Více informací o Radě Evropy naleznete na internetu na adrese http://hub.coe.int.

Další informace týkající se judikatury Evropského soudu pro lidská práva jsou k dispozici na internetových stránkách ESLP (www.echr.coe.int/echr). Vyhledávač HUDOC umožňuje přístup k rozsudkům a rozhodnutím v angličtině a/nebo ve francouzštině, překladům do vybraných jazyků, měsíčníku stručných informací o projednávaných případech, tiskovým zprávám a dalším informacím o práci Soudu.

10.2811/53430
TK-01-13-772-CS-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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). Technologický pokrok rozšiřuje hranice například pro sledování, odposlouchávání komunikací a uchovávání údajů; všechny tyto oblasti představují velké problémy z hlediska práva na ochranu 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 klíčovou judikaturu, shrnuje hlavní rozhodnutí Evropského soudu pro lidská práva (ESLP) i Soudního dvora Evropské unie (Soudní dvůr). V případech, kdy taková judikatura neexistuje, uvádí praktické příklady pomocí hypotetických scénářů. Stručně řečeno, cílem této příručky je pomoci zajistit, aby právo na ochranu údajů bylo prosazováno rázně a s odhodláním.

**AGENTURA EVROPSKÉ UNIE PRO ZÁKLADNÍ PRÁVA**
Schwarzenbergplatz 11 – 1040 Vídeň – Rakousko
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

**EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA**
**RADA EVROPY**
67075 Štrasburku Cedex - Francii
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
www.echr.coe.int – publishing@echr.coe.int

Úřad pro publikace

ISBN 978-92-871-9933-1 (Rada Evropy)
ISBN 978-92-9239-326-7 (FRA)