

Eva Janečková

GDPR

ŘEŠENÍ PROBLÉMŮ V PRAXI OBCÍ

- realizace povinností správce osobních údajů
- dokládání plnění povinností
- nezbytné vnitřní předpisy
- nejčastější pochybení a jejich řešení
- zpracování osobních údajů zaměstnanců



Eva Janečková

GDPR

ŘEŠENÍ PROBLÉMŮ V PRAXI OBCÍ

- realizace povinností správce osobních údajů
- dokládání plnění povinností
- nezbytné vnitřní předpisy
- nejčastější pochybení a jejich řešení
- zpracování osobních údajů zaměstnanců



Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována ani šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude trestně stíháno.

Edice Právo pro praxi

JUDr. Eva Janečková

GDPR – Řešení problémů v praxi obcí

Vydala Grada Publishing, a.s.

U Průhonu 22, 170 00 Praha 7

tel.: +420 234 264 401, fax: +420 234 264 400

www.grada.cz

jako svou 7167. publikaci

Odpovědná redaktorka Ing. Michaela Průšová

Realizace obálky Vojtěch Kočí

Sazba Antonín Plicka

Počet stran 344

První vydání, Praha 2019

Vytiskla tiskárna Tisk Centrum, s.r.o., Moravany

© Grada Publishing, a.s., 2019

ISBN 978-80-271-2718-4 (pdf)

ISBN 978-80-271-2719-1 (ePub)

ISBN 978-80-247-2925-1 (print)

Obsah

Seznam použitých pojmů	9
Seznam zkratek	11
Úvod	13

I. OBECNÁ ČÁST

1 Základní pojmy používané v oblasti ochrany osobních údajů	19
2 Základní zásady Obecného nařízení (GDPR) a jejich odraz v povinnostech	35
2.1 Zásada zákonnosti, korektnosti a transparentnosti	35
2.2 Zásada účelového omezení	40
2.3 Zásada minimalizace údajů	41
2.4 Zásada přesnosti	42
2.5 Zásada omezení uložení	43
2.6 Zásada integrity a důvěrnosti	45
2.7 Zásada odpovědnosti	45
3 Práva subjektu údajů	47
3.1 Právo na informace	48
3.2 Právo na přístup k osobním údajům	66
3.3 Právo na opravu a doplnění	71
3.4 Právo na výmaz	74
3.5 Právo na omezení zpracování	82
3.6 Právo na přenositelnost	84
3.7 Právo vznést námitku	91
3.8 Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování	93
3.9 Právo podat stížnost u dozorového úřadu	99
3.10 Výkon práv	100

4	Souhlas se zpracováním osobních údajů	103
5	Záznamy o činnostech	111
6	Posouzení vlivu na ochranu osobních údajů	115
7	Smlouva o zpracování osobních údajů	123
8	Zabezpečení osobních údajů a jeho porušení	133
8.1	Povinnost zabezpečit osobní údaje	133
8.2	Porušení zabezpečení osobních údajů	139
8.3	Úloha zpracovatele	147
9	Dozorový úřad	149
10	Jmenování pověřence pro ochranu osobních údajů	157
11	Sankce	173

II. ZVLÁŠTNÍ ČÁST

1	Zveřejňování osobních údajů, mlčenlivost	187
1.1	Zveřejňování smluv podle zákona o registru smluv a ochrana osobních údajů ...	189
1.2	Ochrana osobních údajů při poskytování informací	196
1.3	Povinnost mlčenlivosti a ochrana osobních údajů	216
1.4	Zveřejňování na úřední desce	226
1.5	Pořízení a zveřejnění záznamu z jednání zastupitelstva za účelem informování veřejnosti	233
2	Zpracování osobních údajů zaměstnanců obce	239
2.1	Zpracování osobních údajů před vznikem pracovního poměru	243
2.2	Zpracování osobních údajů v průběhu pracovního poměru	254
2.3	Zpracování osobních údajů po skončení pracovního poměru	261
2.4	Ochrana soukromí zaměstnanců na pracovišti	263

3	Video a audio záznamy jako zpracování osobních údajů	271
3.1	Pořizování zvukového a obrazového záznamu účastníkem řízení	277
3.2	Pořizování zvukového a obrazového záznamu ze strany správního orgánu	281
3.3	Kamerový systém uvnitř úřadu	283
3.4	Možnost využití záznamu z kamerového systému ve správním řízení	287
3.5	Městské dohlížecí kamerové systémy	291
3.6	Provozování kamerových systémů v obecních bytových domech	302
4	Zákonný rámec zpracování osobních údajů obecní policií	307
5	Zvláštní činnosti obce	313
5.1	Kroniky obce	313
5.2	Jubilea a gratulace občanům	319
5.3	Správní řízení	323
5.4	Poskytování osobních údajů při kontrole	327
6	Měření rychlosti	329
	Závěr	333
	Seznam použité literatury a materiálů	335

Seznam použitých pojmů

Obecné nařízení (GDPR)	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (General Data Protection Regulation)
osobní údaje	<i>definice podle zákona o ochraně osobních údajů:</i> jakékoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu <i>definice podle Nařízení:</i> veškeré informace o identifikované nebo identifikovatelné fyzické osobě – o subjektu údajů
správce	<i>definice podle zákona o ochraně osobních údajů:</i> každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak. <i>definice podle Nařízení:</i> fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení
subjekt údajů	identifikovatelná fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
souhlas	<i>definice podle zákona o ochraně osobních údajů:</i> svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů <i>definice podle Nařízení:</i> jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů

Porušení zabezpečení osobních údajů	porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů
zákon o ochraně osobních údajů	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
zpracovatel	<i>definice podle zákona o ochraně osobních údajů:</i> každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona <i>definice podle Nařízení:</i> fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
zpracování (osobních údajů)	<i>definice podle zákona o ochraně osobních údajů:</i> jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace <i>definice podle Nařízení:</i> jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
zvláštní kategorie osobních údajů	osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby
adaptační zákon	nový zákon o ochraně osobních údajů, který je ve stádiu návrhu upravuje v souladu s Nařízením některé oblasti specificky pro Českou republiku
Sbor (Skupina WP29)	pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995
dozorový úřad	Úřad pro ochranu osobních údajů
pověřenec (DPO)	osoba dozorující u správce či zpracovatele zpracování osobních údajů
posouzení vlivu (DPIA)	posouzení pravděpodobného rizika zamýšleného zpracování

Seznam zkratk

exekuční řád – zákon č. 120/2001 Sb., exekuční řád, ve znění pozdějších předpisů

kontrolní řád – zákon č. 255/2015 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů

nařízení vlády o katalogu prací – nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě

nařízení vlády o platových poměrech – nařízení vlády č. 341/2017 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě, ve znění pozdějších předpisů

občanský zákoník – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

správní řád – zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

zákon o kronikách – zákon č. 132/2006 Sb., o kronikách obcí

zákon o obcích – zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů

zákon o obecní policii – zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů

zákon o ochraně osobních údajů – zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

zákon o Policii ČR – zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

zákon o přestupcích – zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů

zákon o registru smluv – zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů

zákon o svobodném přístupu k informacím – zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

zákon o úřednicích územních samosprávných celků – zákon č. 312/2002 Sb., o úřednicích územních samosprávných celků a o změně některých zákonů, ve znění pozdějších předpisů

zákon o zaměstnanosti – zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

zákoník práce – zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Úvod

Česká republika má s právní úpravou v oblasti ochrany osobních údajů dlouholeté zkušenosti. Prvním právním předpisem byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl prvním uceleným právním předpisem v oblasti ochrany osobních údajů a který vznikl po přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Uvedený zákon upravil ochranu osobních údajů, zejména povinnosti související s ochranou informací, pouze při provozování informačních systémů nakládajících s osobními údaji. Dále stanovil odpovědnost provozovatelů takových informačních systémů a dalších fyzických a právnických osob účastnících se provádění činností souvisejících s provozováním informačních systémů. Neupravil či upravil pouze částečně řadu dalších oblastí, např. dostatečnou ochranu osobních údajů vypovídajících o osobnosti a soukromí, povinnost toho, kdo shromažďuje osobní údaje, informovat občana o jeho právech a o jiných pro něj významných skutečnostech, oznamovací povinnost nakládání s osobními údaji u kontrolního orgánu subjektem, který hodlá nakládat s osobními údaji, možnost zásahu kontrolního orgánu před zahájením takového nakládání s osobními údaji, které by z hlediska ochrany osobních údajů mohlo představovat určitá rizika, sankce za porušování zákona a předávání údajů do jiných zemí.¹ Tento nedostatek napravil až zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Vzhledem k tomuto stavu nebyl český právní řád, kam byl zmíněný zákon převzat, kompatibilní s právem Evropské unie, na jejíž půdě byla přijata zvláštní Směrnice Evropského parlamentu a rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (dále jen „Směrnice 95/46/ES“), která ukládala členským státům, aby ji promítly do tří let do svých právních řádů. Svoje zákony s ní musely samozřejmě harmonizovat i státy, které se chtěly stát členy Evropské unie.

¹ Důvodová zpráva k zákonu č. 101/2000 Sb., Sněmovní tisk č. 374/0.

Cílem Směrnice 95/46/ES bylo zajistit vysokou úroveň ochrany osobních údajů ve všech členských státech Unie, zajistit volný pohyb informací a informačních služeb mezi členskými státy (zejména z důvodu stále se rozvíjejícího vnitřního trhu), stanovit společný rámec pro práci s osobními údaji a jejich ochranu na území Evropské unie a sladit národní legislativu v této oblasti platnou na území jednotlivých států (členské státy si mohou v národních předpisech upřesnit obecné podmínky a zákonitosti zpracování osobních údajů. Zásady ochrany se měly vztahovat na veškeré zpracování osobních údajů kteroukoliv osobou, jejíž činnosti spadají do oblasti působnosti práva EU (nevztahuje se však na fyzické osoby, které provádějí zpracování osobních údajů, které má výlučně osobní povahu – např. vedení adresáře, korespondence...), musely se vztahovat na veškeré informace týkající se identifikované nebo identifikovatelné osoby (nevztahují se tedy na anonymní nebo anonymizované údaje) a vztahovaly se i na zvukové a obrazové údaje týkající se fyzických osob.

Směrnice však pocházela již z roku 1995, a byla tedy 22 let stará. V těchto letech došlo k prudkému rozvoji informačních technologií, ke změnám v kategoriích nejčastěji zpracovávaných osobních údajů, i k určitému smazání hranic mezi státy. Vzhledem k tomu, že měl každý stát svou vlastní právní úpravu (a navzdory tomu, že všechny zákony vycházely ze Směrnice 95/46/ES), v mnoha oblastech se značně lišily, přinášela tato skutečnost komplikace.

Proto vyvstala potřeba úpravu zmodernizovat a sjednotit. Na základě zkušeností z aplikování Směrnice bylo jako právní forma nové úpravy vybráno nařízení. Nařízení má obecnou závaznost (podobá se vnitrostátnímu zákonu) – upravuje konkrétní situace pro abstraktně určené adresáty. Je závazné ve všech svých částech (nemůže být adresáty aplikováno nahodile a pouze v některých částech). Důležité je především to, že je přímo použitelné v každém členském státě (automaticky zakládá práva a povinnosti v právním řádu členských států). V okamžiku vstupu v platnost platí ve všech členských státech bez ohledu na existenci případných adaptačních zákonů a všechny orgány členského státu, správní úřady i soudy jsou povinny nařízení aplikovat. V okamžiku, kdy nařízení vstoupí v platnost, vytlačuje veškeré vnitrostátní právo, které je s ním v rozporu.

Dne 27. dubna 2016 schválil Evropský parlament konečnou podobu Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Obecné nařízení (GDPR) měly členské země do 6. května 2018 převést do vnitrostátní legislativy, platit začalo od 25. května 2018.

Zároveň byl vytvořen návrh tzv. adaptačního zákona, kterým je návrh zákona o ochraně osobních údajů. „Návrh nového zákona o ochraně údajů má mimo jiné formou adaptace zajistit soulad vnitrostátní právní úpravy s obecným nařízením o ochraně osobních údajů, jehož hlavním cílem je účinná ochrana osobních údajů v celé Evropské unii, která vyžaduje posílení a podrobné vymezení práv subjektů údajů a povinností těch, kdo osobní údaje zpracovávají a o jejich zpracování rozhodují, a dále též rovnocenné pravomoci dozorových úřadů při monitorování a zajišťování souladu s pravidly ochrany osobních údajů, jakož i rovnocenné sankce za jejich porušování v členských státech.

Řádné fungování vnitřního trhu vyžaduje, aby volný pohyb osobních údajů v Evropské unii nebyl omezován z důvodů souvisejících s ochranou osobních údajů fyzických osob. Jednotná úroveň ochrany fyzických osob v celé Evropské unii zamezí rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu a poskytne hospodářským subjektům, včetně mikropodniků a malých a středních podniků, právní jistotu a transparentnost, které fyzickým osobám ve všech členských státech zajistí stejnou úroveň práv vymahatelných právními prostředky a správcům a zpracovatelům uloží povinnosti a úkoly, prostřednictvím důsledného monitorování zpracování osobních údajů a rovnocenných sankcí ve všech členských státech, jakož i účinné spolupráce mezi dozorovými úřady jednotlivých členských států.“²

Také byl vytvořen návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

² Důvodová zpráva k zákonu o zpracování osobních údajů.

I.

OBEČNÁ ČÁST

1 Základní pojmy používané v oblasti ochrany osobních údajů

Jedním z klíčových ustanovení Obecného nařízení (GDPR) je článek 4, v němž jsou vymezeny základní pojmy. Toto ustanovení patří mezi jedno z nejdůležitějších, neboť z pojmů a z jejich aplikace vycházejí veškerá práva a povinnosti, která z Obecného nařízení (GDPR) vyplývají.

Nejprve je nutné přesvědčit se, že informace, s níž správce pracuje, je skutečně osobním údajem ve smyslu definice podle článku 4 písm. a) Obecného nařízení (GDPR), zda proces s ním prováděný je zpracováním ve smyslu definice, a teprve v případě kladné odpovědi na tyto otázky se správce zabývá dalšími ustanoveními Obecného nařízení (GDPR), jež mu ukládají povinnosti a dávají práva.

Článek 4 definuje řadu základních pojmů; vymezeny jsou všechny základní pojmy ve smyslu jejich hmotného obsahu (např. osobní údaj a další) a také pojmy, které lze označit za „popis procesu“ (např. zpracování).

Osobní údaj

Tento pojem je tím nejzákladnějším a nejpoužívanějším pojmem. Definice zůstala téměř stejná jako v předchozí právní úpravě. Podle definice jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Ke změně došlo především v příkladném výčtu osobních údajů ve druhé části definice.

Pojem je definován několika faktory. Prvním faktorem je rozsah. Definice říká, že osobním údajem je informace, aniž by typ informace nějak limitovala. Termín „informace“ jako takový není nijak vymezen, ale ani omezen. Znamená to například, že

není kladen důraz na pravdivost informace. Může se také jednat nejen o informace tzv. objektivní, ale také o různé soudy, hodnocení, závěry a podobně.

Osobním údajem je tedy jakýkoli údaj, jenž se vztahuje k nějaké fyzické osobě. Současně je ovšem třeba, aby tato osoba byla těmito údaji či na jejich základě identifikovatelná. Pro to, zda jde o osobní údaj, je rozhodná skutečnost, zda je možno ze strany správce vytvořit přímý vztah mezi takovým údajem a danou fyzickou osobou. Takový vztah se vytváří prostřednictvím určitých identifikátorů, na jejichž základě lze jednoznačně určit, že se jedná o určitou osobu.

O osobní údaj se však jedná i v případě, že správce sice nedisponuje údaji, jimiž by mohl provést (přímou) identifikaci, ale má možnost si takový údaj opatřit a spojit s údajem, kterým disponuje (např. jméno a příjmení s rodným číslem). V takovém případě lze zjistit identitu subjektu údajů nepřímou. Určenost je tedy stav, kdy správce disponuje údaji, jimiž lze fyzickou osobu přímo jednoznačně identifikovat, o určitelnost jde tam, kdy správce může na základě údajů, která má buď k dispozici, nebo k nimž má přístup, tuto osobu jednoznačně odlišit od jiných subjektů.³ V těchto případech bude nezbytné zpracování takových údajů posuzovat zcela individuálně, případ od případu. Bude záležet na rozsahu údajů či zpracovávaných informací, dostupnosti a legálním zdroji případných dalších údajů, přístupu k těmto zdrojům apod.

Obecné nařízení (GDPR) stanoví, že informace se musí týkat subjektu údajů (tedy fyzické osoby) a tato fyzická osoba pak musí být buď identifikovaná, nebo alespoň identifikovatelná. I když lze jistě polemizovat, které informace mohou subjekt údajů identifikovat, a to natolik přesně, aby nebyla zaměnitelná za jinou fyzickou osobu, lze nepochybně říci, že těmito údaji obecně bude jméno, příjmení, bydliště a případně i rok narození. Na základě těchto údajů bude fyzická osoba identifikována přímo a subjekt údajů tak bude určen. Fyzická osoba však může být identifikována, a tedy určena v některých případech i menším rozsahem údajů. Pak se hovoří o určení nepřímém, tedy identifikovatelnosti, resp. určitelnosti subjektu údajů.

Pojem „osobní údaj“ byl vždy dotvářen rozhodováním soudů.

K otázce, kdy se o osobní údaj nejedná, se například vyjádřil Nejvyšší správní soud (dále jen „NSS“) v rozsudku ze dne 29. 7. 2009, čj. 1 As 98/2008 – 148 tak, že uvedl *„za osobní údaj však zdejší soud nepovažuje ani jméno a příjmení osoby (návštěvníka) ve spojení s číslem jeho občanského průkazu. Ani na základě těchto údajů totiž není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla průkazu. Navíc v případě čísla občanského průkazu se jedná o označení, které je*

³ Mates, P.: Ochrana soukromí ve správním právu. Praha 2004, s. 188.

v průběhu času proměnlivé. Fyzická osoba totiž neobdrží jedno číslo občanského průkazu na celý život, nýbrž při každé výměně tohoto průkazu získává průkaz s číslem novým. Ani ve spojení tohoto čísla se jménem a příjmením fyzické osoby nelze zpravidla zjistit konkrétní identitu, a to tím spíše, jedná-li se o údaje z knihy návštěv vedené na služebně policie v Praze – tj. v místě, kde množina potenciálních návštěvníků je velmi rozsáhlá“.

Nicméně pojem osobní údaj je velmi „tvárný“. Zatímco v jednom případě se o osobní údaj jednat nebude (viz právě rozsudek NSS shora), v jiném případě to platit nemusí a stejná kombinace informací (tedy jméno, příjmení a číslo občanského průkazu) osobním údajem bude. Příkladem může být situace, kdy se tato kombinace údajů dostane např. k Policii České republiky. Ta má oprávněný přístup do evidence občanských průkazů,⁴ a tak jí i tato kombinace informací stačí k tomu, aby fyzická osoba byla minimálně identifikovatelná, což znamená, že v tomto případě se o osobní údaje jednat bude (minimálně tedy ve vztahu k Policii ČR).

V dalším rozsudku NSS byl použit prvek, který je reálným aplikačním rozšířením základní zákonné definice. Tímto prvkem je možnost fyzickou osobu kontaktovat. Tedy jinak řečeno, NSS došel k názoru, že osobním údajem může být i jen samostatně stojící informace o „čísle nebo kódu“.

V rozsudku ze dne 12. 2. 2009, čj. 9 As 34/2008 – 68 totiž dovodil, že, „*plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většinou populace snadno dostupná, ve své podstatě neznámá nic jiného než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu. Proto se výklad pojmu „osobní údaj“ nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou, kulturní nebo sociální identitu (viz shora). Prostřednictvím tohoto čísla je však možno daný subjekt v určitém časovém úseku přímo kontaktovat (což se ostatně stalo i v posuzovaném případě), a tento subjekt je tak dosažitelný a jistým způsobem určitelný, a to případně i bez znalosti jeho jména a dalších údajů, které již vazbu na jeho fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu mají“.*

Ve výše naznačeném smyslu by pak za osobní údaj (alespoň v některých případech) mohla být považována i e-mailová adresa. Jistě si lze představit, že e-mailová adresa

⁴ Ustanovení § 66 odst. 2 zákona o Policii České republiky mimo jiné stanoví, že Policie může v rozsahu potřebném pro plnění konkrétního úkolu žádat od správce evidence nebo zpracovatele poskytnutí informací... agendového informačního systému evidence občanských průkazů.

ve tvaru jmeno.příjmení@firma.cz osobním údajem bude. Ve kmeni je totiž uvedeno komu, které, podle tvaru jednoznačně fyzické osobě, náleží. A ve spojení s označením firmy, jíž zřejmě přísluší daná doména, je taková fyzická osoba identifikovatelná, a tedy o osobní údaje se jednat bude⁵. Obdobné pak bude jistě platit, pokud za @ bude i jen označení poskytovatele (např. tedy seznam.cz)

Jinou kombinací údajů pak posuzoval NSS v případě, kdy se jednalo o informace o „politické příslušnost“ a v jedné své části se týká i toho, zda informace je, či není citlivým osobním údajem, přesněji, zda se jedná o údaj citlivý (dnes zvláštní kategorie údajů), nebo jen o údaj tzv. obyčejný. Jde o rozsudek NSS 3 As 3/2010 – 182, ze dne 26. dubna 2011, který je zajímavý z mnoha důvodů a svým dosahem se dotýká i ústavního práva. V tomto rozsudku se totiž jednalo o to, zda lze, či nelze podle informačního zákona (zákon č. 106/1999Sb., o svobodném přístupu k informacím) poskytnout „seznamy všech soudců působících u obecných soudů v ČR, kteří byli v minulosti členy KSČ“.

Tyto informace tehdy Ministerstvo spravedlnosti odmítlo poskytnout s tím, (cit. z uvedeného rozsudku), „že poskytování informací o politické příslušnosti je citlivým údajem podle § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů (dále též „zákon o ochraně osobních údajů“), a ty je vždy možno shromažďovat a poskytovat pouze s výslovným souhlasem subjektu těchto údajů (§ 9 zákona o ochraně osobních údajů). Shromažďování těchto citlivých údajů nespadá do působnosti Ministerstva spravedlnosti. Ministerstvo ani nevede osobní spisy soudců. Osobní spisy soudců vedou výhradně jednotlivé soudy“.

NSS ve svém rozsudku vycházel z právní názoru vysloveného Ústavním soudem v nálezu ze dne 15. 11. 2010, sp. zn. I. ÚS 517/10 a ve vztahu ke zde traktované problematice dovedl, vycházejí z názoru Ústavního soudu, že „i zde Nejvyšší správní soud musí respektovat princip vázanosti soudů právními názory 3 As 3/2010 – 188 Ústavního soudu s odkazem na čl. 89 odst. 2 Ústavy, a proto vychází z toho, že požadované údaje Ústavní soud kategorizuje jako osobní údaje ve smyslu § 4 písm. a) zákona o ochraně osobních údajů, používající nižší ochrany než tzv. „citlivé údaje“, a na režim jejich zpracovávání dopadá ustanovení § 5 odst. 2 citovaného zákona. Nejvyšší správní soud přitom, má-li se podle imperativu Ústavního soudu v citovaném nálezu stran obdobné věci pohybovat svými úvahami v intencích § 4 písm. a) a 5 odst. 2 zákona o ochraně osobních údajů, a musí vybrat z obsahu ustanovení § 5 odst. 2, potom za jediné v dané věci v úvahu přicházející pravidlo pro zpracovávání předmětných údajů považuje Ústavním soudem doporučené pravidlo zakotvené v písm. f) citovaného ustanovení. Podle

⁵ K podrobnostem o tomto tématu viz Bartík, v. – Janečková, E.: E-mailová adresa jako osobní údaj. In: Daně a právo v praxi 5/2013.

názoru Ústavního soudu ústavně konformní interpretace těchto ustanovení podústavní úpravy umožňuje dospět k závěru, že požadované informace mají být stěžovateli poskytnuty i bez souhlasu dotčených subjektů“.

Také následující judikát pochází z oblasti informačního zákona, ač řeší otázku, co to je, či není osobní údaj. Jde o rozsudek NSS ze dne 13. 8. 2014 čj. 1 As 78/2014 – 41. Dle shrnutí (systém ASPI JUD260495CZ – JUD260495CZ – 1 As 78/2014 – 41 – právní věta) NSS dovodil, že „*žádost o informaci, v níž se žadatel domáhá poskytnutí jmenového seznamu osob, kterým bylo mimořádně uděleno státní občanství České republiky z důvodu, že Ministerstvo vnitra shledalo, že udělení státního občanství těmto osobám by bylo významným přínosem pro Českou republiku [§ 11 odst. 2 písm. d) zákona č. 40/1993 Sb., o nabytí a pozbytí státního občanství], nelze odmítnout s poukazem na ochranu osobních údajů dotčených osob (dle § 15 odst. 1 ve spojení s § 8a zákona č. 106/1999 Sb., o svobodném přístupu k informacím). Poskytnutí takové informace je v souladu s § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, možné i bez souhlasu dotčených osob“.*

V žádosti (adresované Ministerstvu vnitra) požadoval žadatel poskytnutí jmenového seznamu osob, kterým bylo uděleno státní občanství dle § 11 odst. 2 písm. d) zákona č. 40/1993 Sb., o nabytí a pozbytí státního občanství, za léta 2010, 2011 a 2012 (ke dni vyřízení této žádosti). Jinak řečeno, požadoval reálně jen jméno a příjmení, což, jak je dnes již obecně známo, by samo o sobě nestačilo k tomu, aby se jednalo pojmově o osobní údaj. Na základě pouhého jména a příjmení se konkrétní fyzická osoba dá stěží identifikovat či kontaktovat (i když i zde objektivně existují výjimky).

Předmětem sporu bylo podle citovaného rozsudku NSS „*otázka, zda je povinností žalovaného vyhovět žádosti podané podle zákona o svobodném přístupu k informacím a poskytnout stěžovateli jmenový seznam osob, kterým bylo v letech 2010, 2011 a 2012 (do doby podání žádosti) uděleno státní občanství České republiky za použití výjimky podle § 11 odst. 2 písm. d) zákona o nabytí a pozbytí státního občanství. Podle tohoto ustanovení mohl žalovaný prominout podmínku stanovenou v § 7 odst. 1 písm. b) zákona o nabytí a pozbytí státního občanství, pokud měl žadatel o udělení státního občanství na území České republiky povolen trvalý pobyt, oprávněně se zdržoval na území České republiky po dobu nejméně 5 let, měl skutečný vztah k České republice a „udělení státního občanství České republiky by bylo významným přínosem pro Českou republiku zejména z hlediska vědeckého, společenského, kulturního či sportovního.“ Podmínka pro udělení státního občanství České republiky stanovená v § 7 odst. 1 písm. b) citovaného zákona spočívala v povinnosti prokázat, že žadatel nabytím státního občanství České republiky pozbude dosavadní státní občanství, nebo že dosavadní státní občanství pozbyl, nešlo-li o bezdomovce nebo osobu s přiznaným postavením uprchlíka na území*

České republiky. Nutno dodat, že uvedená úprava pozbyla účinnosti dne 1. 1. 2014. Nyní účinný zákon č. 183/2013 Sb., o státním občanství České republiky a o změně některých zákonů, však také upravuje možnost udělení státního občanství České republiky „z důvodu významného přínosu pro Českou republiku“ a oprávnění žalovaného prominout v takovém případě splnění některých zákonných podmínek pro jeho udělení (viz § 16 zákona č. 183/2013 Sb.)“.

Při rozlišení, zda se o osobní údaj jedná a zda jej poskytnout, NSS uvažil, že „v nynějším případě nelze presumovat, že všechny osoby, jejichž soukromí by bylo poskytnutím stěžovatelem požadované informace dotčeno, jsou osobami veřejně činnými. Osoby, kterým bylo uděleno státní občanství z důvodu jejich „významného přínosu pro Českou republiku“, budou velmi pravděpodobně ve většině případů osoby, které lze považovat spíše za veřejně známé (k podrobnému rozlišení mezi osobami veřejně činnými a veřejně známými viz Bartoň, M. Svoboda projev: principy, garance, meze, Praha: Leges, 2010, s. 243–255). Lze si však představit i situace, kdy by občanství mohlo být uděleno na základě předmětné výjimky také osobám, u nichž může být sporný také tento status (typicky v případě excelentního vědce, jehož jméno je známo pouze v úzké komunitě odborníků v oboru, kterému se věnuje)“.

Nakonec došel k závěru, že i zmiňovaná kombinace, tedy jméno a příjmení, ve spojení s informací o poskytnutí státního občanství a veřejné známosti dotčených osob na základě rozlišovacího parametru podle zákona o nabytí a pozbytí státního občanství tedy jejich „významného přínosu pro Českou republiku“ uzavřel, že „otázku, které osoby mají natolik významný přínos pro Českou republiku, aby jim z tohoto důvodu mohlo být mimořádně uděleno státní občanství, je zcela namístě podrobit „ohni veřejné debaty“, neboť je zjevné, že poskytování tohoto speciálního privilegia může být v konkrétních případech značně kontroverzní. Pokud určitá osoba žádá o udělení státního občanství na základě dané výjimky, pak nutně jistým způsobem vstupuje do veřejné sféry a měla by být srozuměna s tím, že bude v budoucnu nucena strpět zásah do svého soukromí spočívající v poskytnutí informace o tom, že předmětným způsobem státní občanství nabyla. Takový omezený zásah do jejího soukromí je nutno považovat za zcela přiměřený“ a uzavírá, že „poskytnutí požadované informace není v rozporu se zákonem na ochranu osobních údajů. Ačkoliv je pravděpodobné, že obsahuje osobní údaje, jejich zpracování (respektive poskytnutí) je v souladu s § 5 odst. 2 písm. e) uvedeného zákona možné i bez souhlasu dotčených osob. Poskytnutí požadované informace tak nelze odmítnout s poukazem na ochranu soukromí (osobních údajů) osob nacházejících se na předmětném seznamu“.

Zajímavým je také rozsudek čj. 5 As 158/2012 – 49 ze dne 23. srpna 2013, který se zabývá pojmem „osobní údaj“ v případě záznamu z kamerového systému. NSS, vycházejí ze základní definice osobního údaje uvedl, že „přímo může být identifikována

osoba zpravidla jménem, nepřímou např. podle telefonního čísla, registračního čísla automobilu, čísla sociálního pojištění, čísla cestovního pasu apod. Nepřímou identifikaci lze provést rovněž pomocí kombinace významných kritérií, která ji umožňují rozeznat zúžením skupiny, do které patří (věk, povolání, bydliště atd.). Z uvedeného vyplývá, že míra dostatečnosti určitých identifikátorů z hlediska provedení identifikace závisí na souvislostech konkrétní situace. Např. běžné příjmení nepostačí k identifikaci, – tj. jednoznačnému určení – osoby v celé populaci země nebo ve velkém městě, ale pravděpodobně bude stačit např. k identifikaci studenta ve třídě nebo ubytovaného hosta v hotelu nebo účastníka konkrétního semináře konaného v daném čase v daném místě. Pokud je se jménem spojeno vyobrazení, může být dokonce možné dozvědět se o vzhledu dané osoby. Všechny nové informace spojené se jménem mohou tedy dovolit „zaostřit“ na konkrétního člověka, a původní informace je tak pomocí identifikátorů spojena s fyzickou osobou, kterou lze odlišit od jiných osob. Zde je třeba poznamenat, že i když je identifikace pomocí jména v praxi nejběžnější, jméno nemusí být nutné pro identifikaci jednotlivce ve všech případech. Tak tomu může být, jsou-li k jednoznačnému určení osoby použity jiné identifikátory.

Co se týče „nepřímou“ identifikovaných nebo identifikovatelných osob, tato kategorie se obvykle vztahuje k jevu „jedinečných kombinací“, ať malého či velkého rozsahu. I v případech, kdy rozsah dostupných identifikátorů prima facie ještě neumožňuje jednoznačně určit konkrétní osobu, může být tato osoba přesto „identifikovatelná“, protože ve spojení s dalšími informacemi (které může, ale nemusí mít v držení správce údajů) tyto informace umožní odlišení daného jednotlivce od jiných osob („jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“ – viz čl. 2 směrnice výše). Některé charakteristiky jsou přitom natolik jedinečné, že lze danou osobu identifikovat velmi snadno (např. prezident, předseda vlády, významné a všeobecně známé osobnosti politického a kulturního života).

Otázka, zda jednotlivce, jehož se informace týká, je, nebo není identifikovaný, tedy závisí vždy na okolnostech daného případu. V tomto kontextu je nutno nahlížet i na provozování kamerového systému „a dále pak uvedl, že „pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. Přitom je třeba zvláště dbát na zohlednění všech faktorů, které v daném případě hrají roli; jedním z faktorů je i zamýšlený účel zpracování a jeho struktura, výhody očekávané správcem údajů, zájmy jednotlivců, které jsou v sázce, ale i riziko organizačních selhání (např. porušení povinnosti zachovávat důvěrnost) a technických problémů.

Jak je uvedeno výše, při posuzování všech prostředků, které mohou být rozumně použity pro identifikaci osob, bude k významným faktorům patřit účel, který správce údajů

zpracováním sleduje. Účelem dohledu pomocí videokamer však je právě identifikace osob zachycených na záznamu ve všech případech, kdy to správce pokládá za nezbytné. Celý systém jako takový se proto musí považovat za zpracovávání údajů o identifikovatelných osobách, i když např. některé natočené osoby v praxi identifikovatelné nemusí být“. K tomu pak NSS konstatoval, že „v již citovaném rozsudku č. j. 2 As 45/2010 – 68, mimo jiné též konstatoval: „Pokud je kamerové snímání prováděno nikoli náhodně, ale systematicky a je-li z něho prováděn záznam, umožňující následně provést identifikaci osoby (§ 3 odst. 4 zákona o ochraně osobních údajů a contrario), jde mimo jakoukoli pochybnost o zpracování osobních údajů [§ 4 písm. a) a e) zákona o ochraně osobních údajů] a tato činnost proto podléhá též reglementaci citovaného zákona“.⁶

O tom, že obsah pojmu „osobní údaj“ není stále definitivně vyjasněn, svědčí rozhodnutí Nejvyššího správního soudu ze dne 17. července 2018, č. j. 3 As 3/2017, v němž se soud zabýval tím, zda protokoly o výpovědích osob v rámci trestního řízení obsahují osobní údaje. Nejvyšší správní soud se při posouzení věci ztotožnil se soudem prvního stupně v názoru, že tyto protokoly je třeba považovat za listiny obsahující osobní údaje vypovídajících osob. Je tomu tak proto, že osoby jsou v protokolech nezaměnitelným způsobem identifikovány, a to jednak jménem, příjmením a funkčním zařazením. Nejvyšší správní soud byl však toho názoru, že osobním údajem je i samotná výpověď osoby.

Nejvyšší správní soud již v rozsudku ze dne 25. 2. 2015, č. j. 1 As 113/2012 – 133 vyložil, že „osobní údaj je tedy jakýkoliv údaj, který se musí týkat fyzické osoby (subjektu údajů) a tato fyzická osoba je nebo může být přímo ze shromážděných údajů nebo na jejich základě jiným způsobem (nepřímo) identifikována“. Poukázal také na bod 26 odůvodnění směrnice 95/46/ES, podle něhož „zásady ochrany se musí vztahovat na veškeré informace týkající se identifikované či identifikovatelné osoby; [...] pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. O osobní údaj tedy nepůjde, jestliže s přihlédnutím ke všem prostředkům, které mohou být rozumně použity možnost určení osoby neexistuje nebo je zanedbatelná.“

V poměrně nedávném rozsudku Soudní dvůr Evropské unie ve věci C-434/16, Nowak proti Data Protection Commissioner jako osobní údaj hodnotil i obsah zkoušky. Vycházel zde přitom z toho, že zkouška směřuje k ověření vysoce osobního a individuálního výkonu zkoušeného, jejím smyslem je zjistit a dokumentovat výkon určité osoby. Obsah zkoušky tak podle Soudního dvora poskytuje informace o osobě zkoušeného. Uvedená východiska se podle názoru Nejvyššího správního soudu tím spíše

⁶ Bartík, V., Janečková.: Pojem osobní údaj ve světle judikatury. In: Daně a právo v praxi 7–8/2015.

uplatní v případě výpovědi osoby v trestním řízení. Taková osoba zde, obecně vzato, poskytuje informace o svém vztahu k věci, která je předmětem trestního řízení. Tato výpověď je poté zdrojem informací o osobě vypovídajícího, má určitou hodnotu i z hlediska věrohodnosti a má své postavení v systému důkazních prostředků. Výpověď je nakonec zaznamenána ve formě protokolu a v takové podobě je možno ji zpracovat. Zdokumentované výpovědi v trestním řízení, tj. nejen identifikační údaje osob, ale tedy i samotný obsah tak nepochybně jsou osobním údajem.

Soud prvního stupně ve svém rozsudku, byť tak učinil stručně, hodnotil protokoly taktéž jako listiny obsahující osobní údaje. Poukázal přitom právě na informační hodnotu obsahu výpovědi osob a dovedl, že z tohoto obsahu je možné určit subjekt údajů.⁷

Obecné nařízení (GDPR) nezná pojem „citlivé osobní údaje“, jak jej obsahoval předchozí zákon. Objevil se termín zvláštní kategorie osobních údajů, jejichž definice však v článku 4 chybí. Tato zvláštní kategorie je upravena v článku 9 Obecného nařízení (GDPR). Tento článek uvádí, že se zakazuje zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Výčet je tedy o něco užší než předchozí definice. Není bez zajímavosti připomenout, že zvláštní význam citlivých osobních údajů (informací) není výsadní doménou právní úpravy ochrany osobních údajů. Jejich význam je jistě zdůrazněn skutečností, že okruhy informací, resp. skutečností se dotýkají těch právních vztahů, jež jsou relevantní např. pro zákaz diskriminace podle zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), když diskriminace je zakázána také z důvodů rasy, etnického původu, národnosti, pohlaví, sexuální orientace, věku, zdravotního postižení, náboženského vyznání, víry či světového názoru⁸.

Je nutné připomenout, že do zvláštních kategorií osobních údajů patří jen ty údaje, které lze zařadit do kategorií, které jsou výslovně zmíněny v článku 9 Obecného nařízení (GDPR). Jiné údaje, byť mohou být lidmi subjektivně považovány jako velmi citlivé, ve smyslu právní úpravy mezi zvláštní kategorie osobních údajů nespadají.

Recitál 53 konstatuje, že zvláštní kategorie osobních údajů, které zasluhují vyšší stupeň ochrany, by měla být zpracovávána pouze pro zdravotní účely, je-li třeba těchto účelů dosáhnout ve prospěch fyzických osob a společnosti jako celku, zejména

⁷ Rozhodnutí Nejvyššího správního soudu ze dne 17. července 2018, č. j. 3 As 3/2017.

⁸ Ustanovení § 2 odst. 3 antidiskriminačního zákona.

v souvislosti s řízením zdravotnických služeb či služeb sociální péče a systémů, což zahrnuje zpracování těchto údajů vedoucími pracovníky a ústředními vnitrostátními zdravotnickými orgány pro účely kontroly kvality, správy informací a obecného vnitrostátního a místního dozoru nad systémem zdravotní nebo sociální péče, a zajištění kontinuity zdravotní nebo sociální péče a přeshraniční zdravotní péče nebo zdravotní bezpečnosti, pro účely monitorování a varování nebo pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely na základě práva Unie nebo členského státu, které musí být ve veřejném zájmu, jakož i pro studie prováděné ve veřejném zájmu v oblasti veřejného zdraví. Proto by toto nařízení mělo stanovit harmonizované podmínky pro zpracování zvláštních kategorií osobních údajů o zdravotním stavu, pokud jde o zvláštní potřeby, zejména je-li zpracování takových údajů prováděno pro určité účely související se zdravím osobou vázanou profesním tajemstvím podle právních předpisů. Právo Unie nebo členského státu by mělo stanovit zvláštní a vhodná opatření s cílem chránit základní práva a osobní údaje fyzických osob. Členské státy by měly mít možnost zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu. To by však nemělo omezovat volný pohyb osobních údajů v rámci Unie, pokud se tyto podmínky uplatní na přeshraniční zpracování takových údajů.

Jedním druhem zvláštní kategorie údajů jsou tzv. biometrické údaje, které Obecné nařízení (GDPR) definuje jako osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

Správce a zpracovatel

Mezi klíčová ustanovení právní úpravy náleží vymezení pojmů správce a zpracovatel. Správcem je podle článku 4 odst. 7 Obecného nařízení (GDPR) fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Jinak řečeno, toto ustanovení jednoznačně charakterizuje okruh adresátů právní normy z hlediska tzv. osobní působnosti a okruhu věcné působnosti. Z výčtu adresátů normy je zřejmé, že nařízení dopadá na každý subjekt, který osobní údaje zpracovává,

neboť vzhledem k rozsahu vymezení těžko nalezneme subjekt, který by byl ze základního vymezení působnosti zákona vyňat, a to bez ohledu na jejich právní subjektivitu.

Správce je každý, kdo určuje prostředky a účel zpracování osobních údajů, přičemž není rozhodné, zda se jedná o fyzickou či právnickou osobu, rozhodná není ani její povaha (může jít o podnikatelský subjekt, orgán veřejné moci či jednotlivce). Významné je, že se dotýčný rozhodl osobní údaje systematicky zpracovávat nebo je mu zpracování uloženo zákonem jako povinnost (např. orgány veřejné správy). Zpracováním osobních údajů může správce provádět sám, nebo může k této činnosti někoho zmocnit nebo pověřit. Touto osobou je zpracovatel, jenž je Obecným nařízením (GDPR) charakterizován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Do definice jsou tak zahrnuty veškeré subjekty bez ohledu na jejich povahu či právní subjektivitu.

Na rozdíl od správce, zpracovatel „pouze“ provádí zpracovávání osobních údajů. Zpracovatel, na rozdíl od správce, neurčuje účel a prostředky zpracování osobních údajů. Zpracovatel nemusí provádět zpracování od začátku do konce, tedy veškeré operace, ale může provádět jen některou (či některé) činnost související se zpracováním. Nemusí tedy jít vždy o subjekt, který osobní údaje shromáždil.

Zpracovatel může zpracovávat údaje buď na základě výslovného zákonného zmocnění, nebo je-li k tomu zmocněn správcem nebo na základě smluvního ujednání. Z dosavadních zkušeností však vyplývá, že vztah mezi správcem a zpracovatelem se v naprosté většině případů odehrává na základě smluvního vztahu.⁹

V některých případech je však stanoveno, že zpracování provádí jiný subjekt, jímž je zpracovatel, přímo zákonem. Takové zákonné zmocnění se obvykle týká jen určitých způsobů zpracování (nejčastěji shromažďování údajů) a správce pak provádí další způsoby (např. uchovávání údajů a jejich předávání).

Z pohledu odpovědnosti za zpracování osobních údajů nelze být zároveň v postavení správce a zpracovatele. Jestliže určitý, např. podnikatelský subjekt, je správcem osobních údajů, nemůže žádná z jeho organizačních složek být současně vůči těmto zpracování těchto osobních údajů zpracovatelem. Případné nesprávné nebo jinak nepřesné používání termínů správce a zpracovatel na postavení a povinnostech podnikatelského subjektu nic nemění.¹⁰

⁹ Bartík, V. – Janečková, E.: Zákon o ochraně osobních údajů s komentářem. Nakladatelství ANAG, Olomouc 2010, s 58.

¹⁰ Poradce č. 3/2005, Zákon o ochraně osobních údajů s komentářem, str. 17.

Subjekt údajů

Dalším důležitým pojmem je pojem subjekt údajů. Zákon o ochraně osobních údajů obsahoval definici, která uváděla, že subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.¹¹

Obecné nařízení (GDPR) samostatnou definici subjektu údajů neobsahuje. Je součástí definice osobního údaje – veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“).

Obecné nařízení (GDPR) se tedy vztahuje pouze na údaje osob fyzických, nikoli osob právnických. Problémy však v minulosti nastávaly u fyzických osob podnikajících. Pohled byl takový, že i fyzická osoba podnikající může být subjektem údajů a jako taková může být zasazena ve svém soukromí, avšak pouze v závislosti na skupině zpracovávaných osobních údajů. Pokud byly zpracovávány pouze osobní údaje týkající se osoby coby podnikatelského subjektu a údaje, které se týkaly pouze její podnikatelské aktivity, nemohlo – vzhledem k tomu, že podnikání není činností, jež by byla s to zasáhnout do soukromí, neboť se netýká soukromí tak, jak jej chápe občanské právo – dojít k neoprávněnému zásahu do soukromí. Takovým údajům proto nebyla přiznána ochrana podle tohoto zákona.

Tento výklad však již byl překonán. Postupně se ukázalo, že většina údajů týkající se fyzických osob podnikajících jakožto podnikatele se překrývá s osobními údaji vztahujícími se k jejich soukromí. Osobní údaje fyzické osoby podnikající jsou proto v současné době považovány za údaje, které požívají ochrany Obecného nařízení (GDPR).

Cílem právní úpravy ochrany osobních údajů je přispět k ochraně soukromí dotčených osob. Právě možný, byť nepřímý, a nikoli významný, resp. bagatelní dopad do soukromí by měl být limitem při rozhodování, zda určitá informace je, či není osobním údajem. Charakter údajů, tedy to, zda vypovídají pouze o soukromém životě dotčené osoby, pouze o profesní činnosti, nebo mají dopad do obou sfér, bude mít význam při posuzování přípustnosti jejich zpracování a míry zásahu, resp. přiměřenosti tohoto zásahu do soukromí dané osoby.¹²

¹¹ Ustanovení § 4 písm. d) zákona o ochraně osobních údajů.

¹² Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J.: GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Wolters Kluwer, Praha 2017, s. 81.

Zpracování

Obecné nařízení (GDPR) dále charakterizuje pojem zpracování, kterým se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Tuto definici lze logicky rozdělit na několik částí. Především říká, že „zpracováním osobních údajů je jakákoliv operace nebo soustava operací“. Definice tak zahrnuje každý zásah do informace. Podstatnou částí této definice je tedy skutečnost, že se nemusí vždy jednat o celý soubor činností, ale může jít v některých případech jen o některé z nich, dokonce se může jednat o operaci jedinou.

K tomu, aby bylo možno hovořit o zpracování, stačí, je-li uskutečňována jen některá z uvedených činností. Výčet je demonstrativní vzhledem k tomu, že s ohledem na vývoj technologií nemohl zákonodárce předvídat, která další zpracování se mohou i v blízké budoucnosti ještě objevit.

Zpracování je tedy operace prováděná s osobními údaji za účelem dosažení cíle, který si stanoví sám správce nebo pro realizaci činnosti, kterou správci ukládá zvláštní zákon. Na druhé straně, ne každý případ, kdy někdo k datům přistoupí, je zpracováním ve smyslu definice. Např. ad hoc přístup k datům nezbytným k servisu poskytovaného hardwaru nebo softwaru nebo jiný zásah do nastavení softwaru či databáze jako takové zpracování osobních údajů ve smyslu definice představovat nebude.¹³

Souhlas

Jedním z nejdůležitějších pojmů pro celou oblast zpracování osobních údajů, je pojem souhlas. Nová definice souhlasu se zpracováním osobních údajů je uvedena v článku 4 odst. 11 Obecného nařízení (GDPR). Podle tohoto ustanovení se souhlasem subjektu údajů rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

¹³ Tamtéž, s. 85.

Ani Obecné nařízení (GDPR) tedy neklade požadavek písemnosti souhlasu se zpracováním osobních údajů. Souhlas musí být konkrétní a jednoznačný. To potvrzuje i recitál 32, který říká, že souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů.

Obecné nařízení (GDPR) zároveň upozorňuje na známou poučku, že mlčení neznamená souhlas, když uvádí, že mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas.

Obecně je poskytnutí souhlasu právním úkonem, a to právním úkonem, který je svým charakterem jednoznačně jednostranným. Nejedná se tedy o dohodu mezi správcem nebo zpracovatelem na straně jedné a subjektem údajů – fyzickou osobou na straně druhé. Pro posouzení jeho platnosti je proto nutné vzít v potaz i úpravu právních úkonů v obecném právním předpisu, jímž je v tomto případě zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“).

Porušení zabezpečení osobních údajů

Obecné nařízení (GDPR) definuje „porušení zabezpečení osobních údajů“ v čl. 4 odst. 12 jako „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.

Co se rozumí pod pojmem „zničení“ osobních údajů, by mělo být zcela jasné: jedná se o situaci, kdy údaje již vůbec neexistují nebo již neexistují ve formě, která je pro správce jakkoli použitelná. Pojem „poškození“ by měl být taktéž poměrně jasný: jedná se o situaci, kdy osobní údaje byly změněny, narušeny nebo již nejsou úplné. Výraz „ztráta“ je nutno v případě osobních údajů vykládat tak, že údaje sice ještě možná existují, ale správce nad nimi ztratil kontrolu, nemá k nim přístup nebo je již nemá ve svém držení. A konečně neoprávněné nebo protiprávní zpracování může zahrnovat zpřístupnění osobních údajů příjemcům, kteří nejsou oprávněni tyto údaje přijímat (nebo k nim mít přístup), (nebo přístup uvedených příjemců k těmto údajům), nebo jakoukoli jinou formu zpracování, která porušuje ustanovení Obecného nařízení (GDPR).

Příklad

Příkladem ztráty osobních údajů může být situace, kdy zařízení obsahující kopii databáze zákazníků správce bylo ztraceno nebo odcizeno. Dalším příkladem ztráty může být situace, kdy jediná kopie souboru osobních údajů byla zašifrována ransomwarem nebo byla zašifrována správcem za použití klíče, který správce již nemá ve svém držení.

Mělo by být jasné, že porušení je druhem bezpečnostního incidentu. Jak však uvádí čl. 4 odst. 12, Obecné nařízení (GDPR) se vztahuje pouze na případy, kdy došlo k porušení zabezpečení osobních údajů. Důsledkem takového porušení je, že správce nebude schopen zajistit dodržování zásad zpracování osobních údajů uvedených v článku 5 Obecného nařízení (GDPR). To poukazuje na rozdíl mezi bezpečnostním incidentem a porušením zabezpečení osobních údajů – zatímco v podstatě všechna porušení zabezpečení osobních údajů představují bezpečnostní incidenty, ne všechny bezpečnostní incidenty jsou nutně porušením zabezpečení osobních údajů.¹⁴

¹⁴ Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679, https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31894

