z právní teorie a praxe

GDPR – revoluce, nebo rozvedení stávajícího?

O obecném nařízení o ochraně osobních údajů – General Data Protection Regulation (dále „GDPR“)[1] bylo již řečeno a napsáno mnohé. V nadcházejících měsících, které zbývají do nabytí jeho účinnosti,[2] uslyšíme o GDPR jistě ještě více. Jako nesprávné ale vnímáme to, že se o tomto nařízení, které má EU poskytnout nový právní rámec ochrany osobních údajů,[3] nehovoří vždy realisticky. Nejčastěji bývá prezentováno jako „revoluce v ochraně osobních údajů“, kterou však v pravém slova smyslu není.

Mgr. Karin Pomaizlová
je advokátkou a partnerkou Taylor Wessing Praha.

Mgr. Monika Fürstová, MBA
je advokátní koncipientkou v Taylor Wessing Praha.

Toto označení kritizuje a na pravou míru uvádí Úřad na ochranu osobních údajů (dále jako „ÚOOÚ“), když říká, že jedním ze základních znaků ochrany osobních údajů je kontinuita.[4] GDPR totiž v cílech i zásadách zpracování a ochrany osobních údajů navazuje na stávající právní úpravu,[5] což konstatuje i vlastní text GDPR např. v čl. 9 recitálu. **Obecné nařízení tedy vychází ze stávající právní úpravy, ale dává si za cíl poradit si se současnou nekonzistentností právní úpravy ochrany osobních údajů v rámci členských států EU. Toho chce docílit prostřednictvím jednotné aplikace jasných pravidel.**

Porovnáme-li obsahově GDPR a směrnici 95/46/ES, dojdeme k závěru, že využívají stejné definice nejdůležitějších pojmů[6] a blízké jsou si i v zásadách zpracování osobních údajů.[7] Zaměříme-li se na pravidla stanovená pro subjekty, které osobní údaje zpracovávají (správce a zpracovatele), zjistíme, že GDPR většinou „pouze“ zpřesňuje a podrobně rozvádí to, co je již ustanoveno ve směrnici 95/46/ES a z. č. 101/2000 Sb., o ochraně osobních údajů, v platném znění (dále jen „ZOOÚ“). V tomto kontextu lze tedy říci, že **GDPR vedle detailnější právní úpravy stávajících povinností správců obsahuje i povinnosti nové** (jako je např. ohlašování případů porušení zabezpečení osobních údajů či jmenování pověřence pro ochranu osobních údajů, viz dále). Podobně je tomu i u práv subjektů údajů**. GDPR rozpracovává práva subjektů údajů, která již mají, a přidává i některé novinky** (např. v podobě práva na přenositelnost údajů[8]). To z této úpravy ještě nečiní revoluci a strašáka podnikatelských subjektů, i když přechod na novou úpravu a její důsledná implementace bude aktivitou náročnou časově i na zdroje. Zejména pro ty

1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, zkráceně obecné nařízení o ochraně osobních údajů.

2 GDPR vstoupilo v platnost dne 27 4. 2016 a účinné (a to přímo) bude od 25. 5. 2018.

3 Nový unijní právní rámec ochrany osobních údajů je vedle GDPR tvořen také ještě směrnicí Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV („JHAD“), a směrnicí Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. 4. 2016 o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti („PNRD“).

4 Viz dokument ÚOOÚ nazvaný „Desatero omylů o obecném nařízení (GDPR)“ dostupný na internetových stránkách úřadu: https://www.uoou.cz/desatero-omylu-o-obecnem-narizeni-gdpr/d-23799/p1=3938.

5 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

6 Porovnej např. definici pojmu „osobní údaj“ v čl. 4 odst. 1 GDPR s čl. 2 písm. a) směrnice 95/46/ES. Obdobně lze porovnat i další klíčové instituty ochrany osobních údajů, jako např. subjekt údajů či zpracování.

7 Porovnej čl. 5 a 6 GDPR s čl. 6 a 7 směrnice 95/46/ES.

8 Skutečnou novinkou v právech subjektů údajů je reálně pouze právo na přenositelnost údajů upravené v čl. 20 GDPR. Ostatní práva subjektů údajů, vč. práva na výmaz – práva být zapomenut – zcela nová nejsou.

subjekty, které dosud ochranu osobních údajů zanedbávaly.

Na revidovaná a přísnější pravidla ochrany osobních údajů lze pohlížet i pozitivně. Občanům (subjektům údajů) mohou poskytnout větší kontrolu nad jejich osobními údaji. **Cílem GDPR je zejména ochránit subjekty údajů ve vztahu k rozvíjející se digitalizaci, profilování uživatelů internetu a sběru velkého počtu dat o nás. Zásadní ale vždy zůstává vymahatelnost povinností.** Každý subjekt by měl postupovat obezřetně a vážit, komu a za jakých podmínek poskytuje osobní údaje. Nejde ani tak o běžný vztah např. zaměstnance a zaměstnavatele nebo o nákupy na internetu. V dnešní době jde spíše o různé aplikace, hry a kvízy, které získávají osobní údaje ze sociálních sítí, a roboty, kteří sledují naši aktivitu na internetu.

GDPR je dobrým podnětem pro podniky, které dosud pravidla ochrany osobních údajů důsledně neimplementovaly, aby si provedly interní audit v oblasti nakládání s osobními údaji, zmapovaly své rezervy a začaly efektivně řešit případné nedostatky v této oblasti. Firmy, které podnikají na úrovni EU, budou profitovat z rovných podmínek, které budou zásluhou GDPR pro všechny subjekty působící v EU (bez ohledu na to, kde se nachází jejich sídlo) shodné. Předpokládán je také pozitivní vliv důvěry v nově nastolovanou ochranu osobních údajů na budování jednotného digitálního trhu jako jedné z hlavních priorit EU,[9] a tím i na (digitální) ekonomiku.[10]

Důvody pro novou úpravu ochrany osobních údajů

I když podstata právní úpravy ochrany osobních údajů včetně základních zásad a klíčových institutů zůstává v GDPR v podstatě stejná jako u směrnice 46/95/ES, byla komplexní revize právní úpravy této oblasti nutná. Jak již naznačují předchozí řádky, **za potřebou aktualizace stojí zejména technologický a společenský vývoj**, v jehož důsledku se stávající právní rámec zřízený směrnicí 95/46/ES[11] stal zastaralým, přestával postupně odpovídat aktuálním požadavkům dnešní doby (době čtvrté průmyslové revoluce) a nezastřešuje již problematiku ochrany osobních údajů dostatečně.[12] V době tvorby (90. léta 20. století) stejně jako v době zavádění tohoto evropského předpisu neexistovaly různé sociální sítě. Existovala např. sice základní myšlenka cloud computingu,[13] ale k vlastnímu poskytování cloudových služeb[14] začalo docházet mnohem později. Nepočítalo se ani s dalšími technologiemi, které jsou dnes více než běžné. Internet věcí[15] existoval nejspíš pouze v hlavách vizionářů a počítačových expertů. V důsledku rozvoje technologií se mění způsoby sběru, využití i přístupnosti dat, včetně osobních údajů. Technický pokrok jde nezadržitelně kupředu, a tak i dnes je již zřejmé, že ani nová regulace představovaná GDPR nepokrývá stoprocentně všechny oblasti ochrany dat. Podle názorů odborníků bude GDPR v době své účinnosti zaostávat za technologickým pokrokem nejméně o pět let.

Z pohledu dnešních zkušeností se jeví, že zvolit pro právní úpravu ochrany osobních údajů na evropské úrovni formu směrnice nebylo šťastné. Právní akt ve formě směrnice totiž sice stanovuje cíl, kterého musí všichni členové EU (během stanovené doby) dosáhnout, ale ponechává na nich způsob, jakým tak učiní. V návaznosti na směrnici 95/46/ES tak vznikly jednotlivé národní právní předpisy (28), které se od sebe více či méně odlišují. To přinášelo firmám nemalé náklady jak časové, tak finanční, jelikož musely dodržovat v rámci podnikání na jednotném trhu EU různé podmínky, které si národní zákony kladly nad rámec směrnice. Taková „volnost" se tedy v oblasti ochrany osobních údajů za stávajících technologických možností jeví jako nevhodná. **Forma nařízení, která byla zvolena pro úpravu novou (GDPR), dává v něm obsaženým pravidlům celounijní platnost. Přímá použitelnost či lépe řečeno účinnost a také závaznost GDPR ve všech členských státech EU bez nutnosti ho do jednotlivých národních právních řádů transponovat si klade za cíl právní úpravu sjednotit a nastolit rovné podmínky pro všechny společnosti, které působí v rámci EU.**

I přes přímou aplikovatelnost GDPR bude ale nezbytné stávající český předpis (z. č. 101/2000 Sb., o ochraně osobních údajů) zásadním způsobem upravit. Ministerstvo vnitra se jako gestor implementace nového právního rámce ochrany osobních údajů rozhodovalo mezi novelizací a přípravou předpisu zcela nového. Nakonec 18. srpna 2017 zveřejnilo návrh zcela nového zákona o ochraně osobních údajů i návrh změn dotčených zákonů.

Základní cíle GDPR

Recitál GDPR definuje základní poslání a záměry nových pravidel ochrany osobních údajů, reprezentovaných zejména tímto nařízením. Obecně má přispět k dotvoření prostoru svobody, bezpečnosti, práva a hospodářské unie. Má směřovat k hospodářskému i společenskému pokroku, posilování a sbližování národních ekonomik. Výsledkem mají být kvalitní životní podmínky. Toho má být specificky dosaženo prostřednictvím sjednocení rozdílů v oblasti ochrany osobních údajů v celé EU, vedoucím k eliminaci rizik v této oblasti, a tedy větší právní jistotě fyzických osob i obchodních společností.

Bude-li dosaženo v rámci EU jednotné úrovně ochrany

9 Tedy zejména digitální trh volný a bezpečný, na němž budou lidé moci nakupovat online bez ohledu na hranice a podniky budou moci prodávat napříč EU bez ohledu na to, ve které její zemi se nacházejí. Podle Komise by plně funkční jednotný digitální trh mohl hospodářství EU každoročně přinést až 415 miliard eur navíc. Součástí evropské strategie zaměřené na digitální trh je právě budování ekonomiky založené na datech a s tím ruku v ruce jdoucí kybernetická bezpečnost. (http://www.consilium.europa.eu/cs/policies/digital-single-market-strategy/).

10 Obsahem pojmu digitální ekonomika je nový a převratný způsob rozdělování zdrojů za intenzivního využití informačních a komunikačních technologií, které vede ke změně struktur řízení podniků a vzniku nových odvětví. Digitální ekonomika úzce souvisí s konceptem informační společnosti a její nedílnou součástí je masová aplikace robotů a automatů ve výrobě i službách.

11 V ČR proveden s účinností od 1. 6. 2000 ZOOÚ.

12 Mj. GDPR vzniklo jako reakce na aféru Edwarda Snowdena, při které vyšlo najevo, že tajné služby USA neoprávněně získávaly osobní informace, a to též o evropských občanech.

13 Cloud computing znamená dodávání výpočetních služeb, jako jsou servery, úložiště, databáze, sítě, software, analytické nástroje a další, a to přes internet (definice viz https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/).

14 Jako cloudovou službu můžeme obecně označit takovou službu, program či aplikaci, která nepracuje lokálně na počítači, ale která je výhradně (nebo z větší části) založena na pomyslném „cloudu", tedy na síti počítačů či serverů umístěných kdesi v kyberprostoru. Cloud je tedy v podstatě synonymem pro internet. Uživatelé pak namísto náročných programů využívají buď jednoduché klientské aplikace, nebo pracují přímo v prostředí svého internetového prohlížeče (viz https://ikaros.cz/cloudove-sluzby-data-i-pocitace-v-oblacich).

15 Internet of Things (IoT) – označení pro moderní přístroje ovladatelné i na dálku pomocí internetu např. prostřednictvím chytrého telefonu. Využití nemusí být omezeno pouze na domácnosti, jde o technologii využitelnou i pro výrobu a průmysl.


Ilustrační foto

podpořené jasnými pravidly pro její vymáhání, povede to k odstranění překážek bránících volnému pohybu osobních údajů, a tedy k rozvoji digitálního trhu a ekonomiky, jak již bylo zmíněno. Profitovat z toho budou jak fyzické osoby, tak ekonomické subjekty.

Základní zásady ochrany osobních údajů

GDPR je založeno na dvou (nových) přístupech:

– **principu odpovědnosti správce za dodržení zásad zpracování**[16] včetně schopnosti shodu se zásadami doložit,[17] a

– **principu rizika**.

Principem rizika se myslí to, že správce od samého počátku zpracování osobních údajů musí brát v úvahu rozsah, kontext, povahu a účel zpracování a zároveň průběžně přihlížet k možným rizikům, která může zpracování znamenat pro práva a svobody fyzických osob. Povinností správce je, aby všem těmto okolnostem přizpůsobil zabezpečení osobních údajů.

Čl. 2 recitálu GDPR zdůrazňuje, že zásady a pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů mají respektovat jejich základní práva a svobody, zejména právo na ochranu osobních údajů.

Základními zásadami zpracování osobních údajů jsou podle GDPR:

– zákonnost,[18]
– správnost a transparentnost,[19]
– účelové omezení,[20]
– minimalizace údajů,[21]
– přesnost,[22]
– omezení uložení,[23]
– integrita a důvěrnost,[24] a
– odpovědnost správce.[25]

Až na poslední zde uvedenou zásadu jsou všechny obsaženy také v ustanoveních směrnice 95/46/ES,[26] a logicky tedy také v ZOOÚ, podle kterého smí správce osobních údajů zpracovávat taková data pouze se souhlasem subjektu údajů,[27] ke stanovenému účelu,[28] pouze v nezbytném rozsahu[29] pro naplnění tohoto účelu a pouze po nezbytnou dobu.[30] Nadto ZOOÚ požaduje, aby osobní údaje získané k rozdílným účelům nebyly sdružovány.[31]

16 Základní zásady zpracování osobních údajů jsou vyjmenovány v čl. 5 GDPR.

17 Např. prostřednictvím kodexu, osvědčení, certifikace nebo vedení záznamů o činnostech zpracování.

18 Požadavek na zákonnost zpracování jako jednu ze zásad je obsažen v čl. 5 odst. 1 písm. a) GDPR a podrobněji pak rozveden v čl. 6 GDPR.

19 Tento požadavek lze vyjádřit také tak, že základem pro zpracování osobních údajů musí být minimálně jeden právní důvod a transparentnost.

20 Viz čl. 5 odst. 1 písm. b) GDPR, který stanoví, že osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmí být dále zpracovávány způsobem, který s nimi není slučitelný. Je vhodné zdůraznit, že osobní údaje mohou být zpracovávány pro různé účely, ale každý takový účel musí být podložen právním důvodem (teprve existuje-li právní důvod zpracování, je správce oprávněn osobní údaje legálně zpracovávat).

21 Viz čl. 5 odst. 1 písm. c) GDPR, který říká, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu zpracování.

22 Viz čl. 5 odst. 1 písm. d) GDPR, který vedle požadavku na přesnost zmiňuje také případné potřeby osobní údaje aktualizovat a povinnost přijmout opatření, která zajistí, aby nepřesné údaje (s přihlédnutím k účelu jejich zpracování) byly bezodkladně opraveny nebo vymazány.

23 Viz čl. 5 odst. 1 písm. e) GDPR, stanovující požadavek na uložení osobních údajů pouze na dobu nezbytnou pro účely zpracování.

24 Viz čl. 5 odst. 1 písm. f) GDPR, který cílí na řádné zabezpečení osobních údajů před neoprávněnými nebo protiprávními zpracováními, před náhodnou ztrátou, zničením či poškozením.

25 Viz čl. 5 odst. 2 GDPR, který správci osobních údajů stanovuje odpovědnost za dodržování zásad zpracování, které navíc musí být schopen doložit.

26 Zejména v čl. 6 směrnice 95/46/ES.

27 Viz ust. § 5 odst. 2 ZOOÚ [definice souhlasu subjektu údajů jako svobodného a vědomého projevu vůle obsahujícího souhlas se zpracováním osobních údajů viz ust. § 4 písm. n) ZOOÚ]. Poskytnutí souhlasu subjektu údajů se zpracováním jeho osobních údajů je provázáno s informační povinností správce osobních údajů vůči jejich subjektu.

28 Zejména viz ust. § 5 odst. 1 písm. a) a f) ZOOÚ, přičemž ZOOÚ rovněž stanovuje informační povinnost správce osobních údajů, jejíž součástí je také informování subjektu údajů o účelu jejich zpracování.

29 Viz ust. § 5 odst. 1 písm. d) ZOOÚ.

30 Viz ust. § 5 odst. 1 písm. e) ZOOÚ.

31 Viz ust. § 5 odst. 1 písm. h) ZOOÚ.

Zákonnost

Správce vyhoví požadavkům zásady zákonnosti, pokud v odpovídajícím rozsahu splní alespoň jednu z podmínek danou čl. 6 odst. 1 GDPR:

– získá souhlas subjektu údajů se zpracováním jeho osobních údajů pro jeden či více konkrétních účelů;[32]

– zpracování je nutné pro jednání o smlouvě nebo plnění smlouvy uzavřené se subjektem údajů;[33]

– zpracování je nezbytné pro splnění právní povinnosti správce;[34]

– zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů či jiné fyzické osoby;

– zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;[35]

– zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany s výjimkou případů, kdy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů.[36]

Transparentnost a odpovědnost

Aby zpracování osobních údajů bylo možné považovat za transparentní,[37] **je třeba, aby správce zpracovával osobní údaje otevřeně, nezatajoval důvody, proč potřebuje osobní údaje zpracovávat (účely zpracování), a také, aby plnil svou informační povinnost vůči subjektům údajů**.[38] Povinností správce je zajistit, aby subjekt údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem, za použití jasných a jednoduchých jazykových prostředků získal veškeré potřebné informace o zpracování jeho osobních údajů, jako je identifikace správce a jeho případného zástupce,[39] účel a právní základ zpracování,[40] příjemce osobních údajů, úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a případně také informace o době uložení osobních údajů, o právu na přístup k osobním údajům, možnost podat stížnost u dozorového orgánu, možnost odvolat udělený souhlas, o právu na opravu, omezení zpracování, či dokonce výmaz atd. Jsou-li osobní údaje získávány přímo od subjektu údajů, poskytuje správce příslušné informace v okamžiku získání osobních údajů.

S transparentností se také úzce pojí již zmiňovaný princip odpovědnosti. **Transparentnost má vést k uvědomění si, že zpracování osobních údajů může zasáhnout a více či méně zasahuje do života fyzických osob a v důsledku nedostatečné ochrany může mít na tyto osoby (negativní) dopad.** K takovému uvědomění má dojít nejen na straně správců, ale také na straně subjektů údajů, které v současné době nejeví dostatečný zájem o to, jak je s jejich daty (v zásadě poskytovanými na každodenní bázi) nakládáno, a tedy ani nevyvíjejí žádný tlak na správce. GDPR by podle Evropské komise tuto situaci mohlo začít měnit.

Práva subjektů údajů

Jedním z cílů GDPR je **posílit práva subjektů údajů**. Toho má být dosaženo prostřednictvím podrobnější a propracovanější úpravy již prověřených institutů a též prostřednictvím zakotvení a úpravy institutů nových. **Konkrétně GDPR stanovuje subjektům údajů:**

- právo na přístup k osobním údajům (viz čl. 15 GDPR),[41]
- právo na opravu a doplnění neúplných osobních údajů (viz čl. 16 GDPR),[42]
- právo na výmaz, resp. právo být zapomenut (viz čl. 17 GDPR),
- právo na omezení zpracování (čl. 18 GDPR),
- právo na přenositelnost údajů (viz čl. 20 GDPR), a
- právo vznést námitku (viz čl. 21 GDPR).

Právo na přístup k osobním údajům

Subjekt údajů má právo na to, aby mu správce potvrdil, zda zpracovává jeho osobní údaje, a pokud ano, má právo získat přístup k nim i k informacím, které se tohoto zpracování týkají. Je-li subjekt údajů dobře obeznámen se skutečností, že jsou jeho data zpracovávána, může pak samozřejmě realizovat i další práva s nimi spojená, jako je právo na opravu či doplnění, právo na přenositelnost údajů a další. Má své osobní údaje pod kontrolou a může s nimi podle vlastního uvážení nakládat.

V současné době je toto právo subjektu údajů zakotveno i v **§ 12 ZOOÚ**. Správce je na žádost subjektu údajů povinen poskytnout mu informaci o zpracování jeho osobních údajů bez zbytečného odkladu.

32 Souhlas subjektu údajů se zpracováním jako základní legální titul zpracování osobních údajů zná ochrana osobních údajů i nyní. Je obsažen v ust. § 5 odst. 2 ZOOÚ. Pro zpracování osobních údajů bez souhlasu subjektu údajů je v ust. § 5 odst. 2 písm. a) až g) ZOOÚ stanoveno pouze několik výjimek, které v zásadě korespondují s čl. 6 odst. 1 GDPR (jde např. o zpracování nezbytné pro dodržení právní povinnosti správce nebo k ochraně životně důležitých zájmů subjektu údajů či pro plnění smlouvy uzavřené se subjektem údajů aj.). Pokud si však správce nezajistí souhlas subjektu údajů se zpracováním a ani na takové zpracování nelze aplikovat zde zmíněné výjimky, je nepochybné, že správce nesplnil jeden ze základních požadavků kladených na zákonné zpracování osobních údajů nyní (podle ZOOÚ) a ani v budoucnu (za účinnosti GDPR).

33 Např. pracovní smlouva či kupní smlouva, ale i jiné.

34 Např. povinnost správce odvádět za svého zaměstnance platby sociálního zabezpečení. Tato povinnost musí být stanovena buď právem EU, nebo právem členského státu EU, které se na správce vztahuje.

35 Tato povinnost musí být stanovena buď právem EU, nebo právem členského státu EU, které se na správce vztahuje (viz čl. 6 odst. 3 GDPR).

36 Zvláště je-li subjektem údajů dítě.

37 Viz čl. 12 a násl. GDPR.

38 Čl. 12 odst. 1 ve spojení s čl. 13 a 14 GDPR. Základní povinnost informovat subjekt údajů o tom, pro jaký účel zpracování a k jakým osobním údajům, jakému správci a na jaké období při udělení souhlasu, stanovuje také stávající česká právní úprava ochrany osobních údajů – ZOOÚ (viz ust. § 5 odst. 4).

39 Případně vč. kontaktu na pověřence pro ochranu osobních údajů, je-li v souladu se čl. 37 GDPR ustanoven.

40 Vč. oprávněných zájmů správce, jde-li o zpracování založené na čl. 6 odst. 1 písm. f) GDPR.

41 Právo na přístup k informacím není novou záležitostí. Je obsaženo i v současné právní úpravě, a to jak ve směrnici 95/46/ES (čl. 12 v souvislosti s recitály 41-43), tak v z. č. 101/2000 Sb., o ochraně osobních údajů, v platném znění (konkrétně ust. § 12 a 21 s tím, že povinnost správce informovat subjekt údajů o jeho právu na opravu osobních údajů je obsažena v ust. § 11 téhož zákona).

42 Také právo na opravu je již součástí stávající legislativy, konkrétně je obsaženo v recitálech 38 a 25 a čl. 6, 10 a 12 směrnice 95/46/ES. Ust. § 5 odst. 1 písm. c), § 11 odst. 1 a § 21 odst. 1 písm. b) z. č. 101/2000 Sb. též referuje k tomuto právu.

Právo na opravu

Právo na opravu je provedením zásady správnosti. Jeho obsahem je **povinnost správce bez zbytečného odkladu opravit nepřesné osobní údaje konkrétního subjektu údajů a neúplné osobní údaje s přihlédnutím k účelu zpracování doplnit**.

S neaktuálními, nepřesnými nebo neúplnými informacemi se stávající právní úprava vypořádává v **§ 5 odst. 1 písm. a) ZOOÚ**, který správci dává za povinnost zpracovávat pouze přesné osobní údaje, a je-li to nezbytné, aktualizovat je. Pokud správce zjistí, že zpracovává údaje, které této podmínce nevyhovují, musí provést příslušná přiměřená opatření, jako je blokování zpracování a oprava či doplnění osobních údajů. Pokud by to nebylo možné, je povinen takové osobní údaje zlikvidovat.[43] Informaci o blokování, opravě, doplnění či likvidaci správce povinně bez zbytečného odkladu sdílí se všemi příjemci.

Právo na výmaz – právo být zapomenut

Právo být zapomenut stejně jako právo na přístup k osobním údajům a právo na opravu existovalo již před přijetím GDPR,[44] bylo založeno směrnicí 95/46/ES, ze které je dovodil[45] Soudní dvůr EU (velký senát) v rozsudku ze dne 13. 5. 2014, ve věci C-131/12, *Google Spain SL, Google Inc. proti Agencia Espa ola de Protección de Datos (AEPD)*. Pan Mario Costeja Gonzáles si přál vymazat internetový novinový článek, který obsahoval informaci z roku 1998 o nuceném prodeji jeho nemovitosti z důvodu dluhu na sociálním pojištění, který však byl následně uhrazen. Se svou žádostí namířenou proti internetovému deníku La Vanguardia a proti Google Spain SL a Google Inc. kontaktoval španělský úřad pro ochranu osobních údajů (AEPD). Vzhledem k výjimce z ochrany osobních údajů pro účely žurnalistiky nebo uměleckého a literárního projevu obsažené ve španělské legislativě však úřad stížnost v části namířené proti elektronickým novinám zamítl. V části proti společnostem Google jí však vyhověl s tím, že jim uložil povinnost odstranit Gonzálesovy osobní údaje z jejich indexu a zabránit budoucímu přístupu k nim.

V rámci rozhodování tohoto sporu vznesl španělský Nejvyšší soud na Soudní dvůr EU (dále jako „SDEU“) předběžné otázky na místní a věcnou působnost směrnice 95/46/ ES a na vlastní výklad práva „být zapomenut“. SDEU vyložil příslušná ustanovení směrnice 95/46/ES[46] tak, že činnost vyhledávačů[47] je třeba jednoznačně považovat za zpracování osobních a jiných údajů ve smyslu směrnice 95/46/ES. Dále se vyslovil v tom smyslu, že provozovatele internetového vyhledávače považuje za správce osobních údajů,[48] a je tedy za jejich zpracování prostřednictvím poskytované služby také odpovědný. Soud dále prostřednictvím širokého výkladu pojmu zpracování osobních údajů odvodil, že ustanovení směrnice 95/46/ES dopadají na činnost vyhledávače Google i přes skutečnost, že Google Inc. je americkou právnickou osobou, není veřejně známo, kde se nacházejí její servery, na kterých jsou data uložena, a madridská pobočka se zabývá „pouze“ reklamou, podporou prodeje a marketingem. SDEU dospěl k závěru, že i když nelze jednoznačně říci, že místem zpracování údajů je oblast EU, zaměřuje se Google na obyvatele členského státu EU a zpracovávání osobních údajů prostřednictvím vyhledávače Google podléhá právní úpravě směrnice 95/46/ES. Co se týče práva být zapomenut, SDEU dovodil, že s ohledem na účel zpracování a plynutí času se může původní zákonné zpracování dat dostat do rozporu s ustanoveními směrnice 95/46/ES. **V případě, že dříve zpracované údaje již nejsou nezbytné pro účely, pro které byly shromažďovány či zpracovávány, mohou se zdát nepřiměřenými nebo nepodstatnými a jejich subjekt požádá o jejich odstranění, musí mu provozovatel vyhledávače vyhovět.** Toto právo subjektu údajů a povinnost správce zpracovávaných dat jsou omezeny možnou převahou zájmu veřejnosti mít k dané informaci při internetovém vyhledávání přístup. Provozovatel vyhledávače je osobou, které náleží právo i povinnost posoudit důvodnost (zákonnost) žádosti subjektu údajů o výmaz informace. Musí přitom přihlížet jak k právu subjektu údajů na ochranu soukromí, tak k právu veřejnosti na přístup ke konkrétní informaci jako výsledku vyhledávání.

Od 25. 5. 2018, kdy GDPR vstoupí v účinnost, již nebude dovozování práva být zapomenut nutné. Právo na výmaz je totiž v čl. 17 GDPR přímo zakotveno. Podle čl. 17 odst. 1 GDPR má subjekt údajů právo, aby správce jeho osobní údaje vymazal, přičemž správce má povinnost tak bez zbytečného odkladu učinit, pokud je dán alespoň jeden z důvodů stanovených v čl. 17 odst. 1 písm. a) až f) GDPR (např. osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny a zpracovávány; subjekt údajů odvolá svůj souhlas se zpracováním a neexistuje žádný další právní důvod pro zpracování; subjekt údajů vznese námitky proti zpracování, v neposlední řadě může být důvodem protiprávnost zpracování). Čl. 17 odst. 2, který hovoří o situaci, kdy byly osobní údaje správcem zveřejněny, má vazbu na prostředí internetu. Jeho podstatou je ochrana osobnosti před negativními následky publicity spočívajícími v tom, že každý člověk má právo požádat internetové vyhledávače,[49] aby se postaraly o odstranění vý-

43 Nepřesné osobní údaje či neúplné osobní údaje mohou být zpracovávány, pouze jsou-li nezbytné pro splnění povinností správce stanovených zvláštními zákony pro zajištění bezpečnosti ČR, obrany ČR, veřejného pořádku a vnitřní bezpečnosti, prevence, vyhledávání a odhalování trestné činnosti a stíhání trestných činů, významného hospodářského zájmu ČR nebo EU, významného finančního zájmu ČR nebo EU, výkonu kontroly a regulace spojených s výkonem veřejné moci, činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti nebo činností spojených s vedením centrální evidence účtů (výjimka viz ust. § 3 odst. 6 ZOOÚ).

44 A to i přesto, že není samozřejmou součástí národních úprav členských států EU. Směrnice 95/46/ES v čl. 9 připouštěla, aby jednotlivé členské státy EU přijaly ohledně práva být zapomenut odlišnou úpravu. Konkrétně Španělsko do svého právního řádu začlenilo výjimku z ochrany osobních údajů pro zpracování osobních údajů pro účely žurnalistiky, uměleckého nebo literárního projevu.

45 Právo být zapomenut není ve směrnici 95/46/ES výslovně zakotveno a bylo dovozeno soudním výkladem.

46 Pracovní skupina WP29 pak v souvislosti s rozsudkem ve věci C-131/12 připravila návod, jak s názory a závěry SDEU v něm obsaženými prakticky pracovat, jak je uplatňovat: viz http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf).

47 Činnost vyhledávačů definovaná jako automatické, nepřetržité a systematické prozkoumávání internetu s cílem vyhledávat zveřejněné informace, které jsou dále indexovány, uspořádávány, uchovávány na serverech provozovatele, a nakonec zpřístupňovány uživatelům jako výsledky jejich vyhledávání.

48 Provozovatel internetového vyhledávače je správcem osobních údajů, neboť sám určuje účel i prostředky zpracování a také zpracování sám provádí.

49 Resp. společnosti, které poskytují službu umožňující v internetové síti vyhledat weby, které nejlépe korespondují s konkrétním uživatelským dotazem – zadaným klíčovým slovem či slovním spojením vystihujícím požadované informace.

sledků vyhledávání,[50] ve kterých je obsaženo jeho jméno.[51]

Proces realizace práva být zapomenut, zejména jde-li o výmaz informací zveřejněných online, není ale zcela jednoduchý. Začíná žádostí dotčené osoby o výmaz. K odstranění nechtěných informací však nedochází automaticky. Každá individuální žádost[52] musí být zvážena, posouzena a odborní pracovníci společnosti provozující daný internetový vyhledávač rozhodnou, zda jí bude vyhověno. Předmětem posouzení je zejména skutečnost, zda je v konkrétním případě vhodné upřednostnit právo jednotlivce být zapomenut před právem veřejnosti na informace.

Právo subjektu údajů na výmaz jeho osobních údajů má své hranice a omezení.[53] Je limitováno výkonem práva na svobodu projevu a informace, plněním povinnosti vyžadující zpracování osobních údajů ve veřejném zájmu či výkonu veřejné moci, nezbytností zpracování osobních údajů pro účely archivace ve veřejném zájmu a pro účely vědeckého nebo historického výzkumu a pro účely statistické a také pro určení, výkon nebo obhajobu právních nároků. Vzhledem k celé řadě výjimek, kterými GDPR výkon práva být zapomenut omezuje, je nasnadě otázka jeho uplatnění a skutečného vymáhání.

Právo na omezení zpracování

Čl. 18 GDPR upravuje právo subjektu údajů, aby v taxativně vyjmenovaných případech správce omezil zpracování jeho osobních údajů. Jde o případy, kdy **subjekt údajů popírá přesnost zpracovávaných osobních údajů, nebo když jde o zpracování protiprávní a subjekt odmítá jejich výmaz a místo toho žádá o omezení jejich použití**. Dále se jedná o situace, kdy správce již údaje pro účely zpracování nepotřebuje, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků. Zpracování osobních údajů může být také dočasně omezeno, pokud proti němu subjekt údajů vznesl námitku a správce nebo zpracovatel prověřují, zda převažují oprávněné důvody na jeho straně nad důvody subjektu údajů.

Dnes obdobnou úpravu obsahuje i ZOOÚ, podle **§ 21 ZOOÚ** má subjekt údajů mj. **právo žádat blokaci svých osobních údajů**, pokud se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem.[54]

Právo na přenositelnost údajů

Subjekt údajů (fyzická osoba) má **právo získat bezplatně**[55] **své osobní údaje, které poskytl správci, a také právo tyto údaje bez omezení předat jinému správci**. Je-li to technicky proveditelné, má subjekt údajů právo na předání svých osobních údajů přímo mezi samotnými správci. V čl. 20 GDPR **nalezneme podmínky, za kterých subjekt údajů toto své právo nabývá:**

– jedná se o osobní údaje (poskytnuté subjektem údajů);
– tyto osobní údaje jsou zpracovávány automatizovaně;
– k jejich zpracování dochází pro konkrétní účely;
– subjekt údajů, který osobní údaje poskytuje, musí s jejich zpracováním předem udělit souhlas nebo musí jít o zpracování nezbytné pro splnění smlouvy, jejíž je subjekt údajů smluvní stranou. Výkonem práva na získání osobních údajů nesmí být negativně ovlivněna práva a svobody třetích stran.

Ustanovení o portabilitě dat správci předepisuje, aby údaje poskytl subjektu údajů v běžně používaném a strojově čitelném formátu.

Je vhodné zdůraznit, že uplatnění práva jednotlivce na přenositelnost údajů neznamená automaticky ukončení vzájemných vztahů či spolupráce, není ani důvodem pro samočinný výmaz dat ze systémů správce. Subjekt údajů může i po přenosu dat efektivně využívat služby správce původního.

V praxi nejčastěji půjde o přenos dat mezi nejrůznějšími aplikacemi, jako jsou např. běžecké či jiné sportovní platformy, hudební platformy, sdílené kalendáře, elektronická pošta, vyhledávače zaměstnání, aplikace shromažďující informace o zdravotním stavu, platformy umožňující seznámení, úložiště fotografií apod.

Přenositelnost údajů je zcela nové právo vytvořené EU k podpoře konkurence na digitálním trhu. Jeho aplikace v praxi již nyní vyvolává řadu otázek. Proto se problematikou přenositelnosti dat, resp. výkladem příslušných ustanovení podrobněji zabývá pracovní skupina WP29.[56] Ta na konci loňského roku zveřejnila svá výkladová stanoviska, která, i když nejsou právně závazná, mají jako právní názor kontrolního orgánu zásadní význam. Jedno z nich je právě také věnované institutu práva na přenositelnost vlastních, správci poskytnutých osobních údajů.[57]

K účelu práva na přenositelnost údajů WP29 uvádí, že ***„dává subjektům údajů možnost obdržet své údaje (ve strukturovaném, běžně používaném a strojově čitelném formátu) a znovu je použít pro vlastní účely a napříč různými službami, usnadní***

50 Jde o odstranění odkazů na stránky s citlivými osobními informacemi, které mohou (negativně) ovlivnit pověst konkrétní osoby. Žádosti se týkají nejrůznějších typů obsahu, včetně záznamů o závažných trestných činech, trapných fotografií, případů internetové šikany a urážení, nejrůznějších starých obvinění, negativních zpravodajských článků atd.

51 Jedná se tedy, stručně řečeno, o právo na to, aby za určitých okolností byly osobní údaje konkrétní osoby vymazány z internetového prostředí, a tak vlastně zapomenuty.

52 Google dokonce připravil pro subjekty údajů, které chtějí právo na výmaz, právo být zapomenut realizovat, online formulář příslušné žádosti. V českém jazyce dostupný na internetových stránkách Google: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=cs.

53 Viz odst. 3 čl. 17 GDPR.

54 Ust. § 21 odst. 1 ZOOÚ: „(1) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může a) požádat správce nebo zpracovatele o vysvětlení, b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.“ Dále ust. § 21 odst. 5 ZOOÚ říká: „(5) Správce je povinen bez zbytečného odkladu informovat příjemce o žádosti subjektu údajů podle odstavce 1 a o blokování, opravě, doplnění nebo likvidaci osobních údajů. To neplatí, pokud je informování příjemce nemožné nebo by vyžadovalo neúměrné úsilí.“

55 Čl. 12 odst. 5 GDPR. Poplatek může být uložen jen v případě zjevně nedůvodných či nepřiměřených např. opakujících se (nadměrně zatěžujících) žádostí.

56 The Article 29 Data Protection Working Party. Tuto pracovní skupinu ustavil čl. 29 směrnice 95/46/ES a je nezávislým evropským poradním orgánem ve věcech ochrany dat a soukromí. Sestává ze zástupců vnitrostátních orgánů pro ochranu údajů, EDPS (European Data Protection Supervisor) a Evropské komise. Její úkoly blíže definuje čl. 30 směrnice 95/46/ES a čl. 15 směrnice 2002/58/ES. Funkce WP29 později převezme Evropský sbor pro ochranu osobních údajů (EDPB – European Data Protection Board) ustavený čl. 68 GDPR.

57 Dokumenty vydané WP29 k právu na přenositelnost dat jsou dostupné na internetových stránkách ÚOOÚ. https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=21750&n=pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich-udaju.

jim přenášet, kopírovat nebo předávat osobní údaje bez jakýchkoliv zábran z jednoho IT prostředí do jiného. To posiluje pozici subjektů údajů jako spotřebitelů (nemusí již zůstávat u jednoho poskytovatele), a v podstatě tak dostávají možnost spravovat si své údaje samy či je přenášet od jednoho správce k jinému, aniž by tomu původní správce mohl nějak bránit."[58]

Z pohledu správce osobních údajů to, pokud provádí zpracování osobních údajů automatizovaně, zejména znamená nutnost být technicky připraven kdykoliv a kterémukoliv subjektu údajů poskytnout jeho osobní údaje, které zpracovává, v přiměřeném formátu, který umožnuje přenos a další použití těchto údajů. V této souvislosti WP29 správcům doporučuje, aby pro subjekty údajů měli připravenu možnost přímého stažení jejich údajů a možnost jejich přímého přenosu k jinému správci. K tomu podle WP29 může být využito rozhraní pro programování aplikací (Application Programming Interface, API). Jiným řešením je uložení a uchovávání osobních údajů jejich subjektem na důvěryhodných úložištích třetích stran. Subjekt údajů pak správcům „jen" povolí přístup ke svým osobním údajům a udělí jim souhlas se zpracováním.

Výkladové pokyny WP29 hovoří o povinnosti správců informovat subjekty údajů o jejich právu na přenositelnost dat, a to jednoduchým, stručným a jasným způsobem. Dále je správcům doporučováno, aby jednoduchým a srozumitelným způsobem vysvětlovali subjektům údajů rozdíly mezi různými typy údajů, které mohou při výkonu práva na přenositelnost obdržet. Vždy půjde o osobní údaje subjektu údajů, a pouze ty, které subjekt údajů správci sám poskytl.

WP29 správcům doporučuje, aby si vytvořili vhodné postupy, které subjektu údajů umožní podání žádosti o přenos údajů a také získání jeho dat. Součástí takového postupu musí být také spolehlivé ověření totožnosti žadatele o přenos dat. To by však neměl být problém, jelikož takové postupy již správci zaváděli u práva na likvidaci osobních údajů. V případě online aplikací mají subjekty údajů, např. uživatelé sociálních sítí, přístup ke svým osobním údajům pomocí unikátního log-in jména a hesla. Není tedy třeba vytvářet nic nového a zvláštního pro potřeby ověření totožnosti subjektu údajů žádajícího o přenos svých osobních dat.

WP29 ve stanovisku vyjadřuje svůj názor a doporučuje správcům dat vykládat pojem „osobní údaje týkající se subjektu údajů" extenzivním způsobem, a to v případech, kdy subjektem údajů vyžádaná data zpracovávaná správcem obsahují také informace o třetích osobách a subjekt údajů je bude využívat pro své osobní účely. Jako příklad takových datových souborů uvádí WP29 záznamy o příchozích a odchozích telefonních hovorech či historii bankovního účtu, zahrnující příchozí i odchozí platební transakce. Dalším příkladem může být přenos souboru fotografií umístěných subjektem údajů na některé ze sociálních sítí. I když jsou na fotografiích kromě subjektu údajů třetí osoby, může si je subjekt údajů vyžádat a může si vyžádat také jejich přenos k jinému správci údajů. Zároveň WP29 v takovém případě zdůrazňuje, že tyto údaje přenášené k novému správci nesmí být zpracovány pro účely tohoto správce a nakládání s nimi musí zůstat subjektu, který přenos dat inicioval (subjektu údajů).

Široký výklad spočívá rovněž ve výkladu termínu „poskytnout". Jde o to, že při poskytování osobních údajů nemusí jít pouze o informace poskytnuté a zadané vědomě a aktivně subjektem údajů, ale může jít také o údaje získané prostřednictvím využívání určité služby či zařízení (např. polohu určenou chytrým telefonem). Naopak takovým údajem nemohou být data odvozená z údajů poskytnutých jejich subjektem (např. uživatelský profil vytvořený analýzou základních dat z chytrého měření). Na taková data se pak právo přenositelnosti nevztahuje (nebyla poskytnuta subjektem údajů) a správci nejsou povinni je subjektům údajů poskytovat.

GDRP upravuje přenositelnost osobních údajů a správci nyní řeší praktickou stránku věci, aby byli od května 2018 schopni nově nastaveným povinnostem vyhovět. Až praktické aplikace ustanovení GDPR ukáží veškeré možnosti komerčního využití práva na přenositelnost dat a jeho impakt na vývoj evropského digitálního trhu. Nechme se tedy překvapit konkrétními technickými řešeními správců osobních údajů a též zájmem, jak na straně subjektů údajů o to svá data přenášet k jiným správcům, tak na straně správců takové osobní údaje přebírat i třeba z důvodů kybernetické bezpečnosti.

Právo vznést námitku

GDPR dává subjektu údajů možnost vznést námitku proti zpracování jeho osobních údajů nejen pro účely přímého marketingu,[59] ale z důvodů konkrétní situace také v případě zpracovávání prováděného ve veřejném zájmu nebo výkonu veřejné moci, kterým je správce pověřen, nebo pro účely oprávněných zájmů správce či třetí strany,[60] a to kdykoliv. Pokud jde o zpracování osobních údajů pro marketingové potřeby, nebudou pak jeho osobní údaje již dále zpracovávány. Stejného výsledku lze v současné době docílit odvoláním souhlasu se zpracováním osobních údajů.

Povinnosti správců osobních údajů

GDPR staví na stejných zásadách jako směrnice 95/46/ES, které podrobněji rozpracovává a dále na nich buduje nové povinnosti spočívající ve vedení záznamu o činnostech zpracování, posuzování vlivu zpracování na ochranu osobních údajů, v konzultacích s dozorovým úřadem, ohlašování porušení zabezpečení osobních údajů (úřadu dozoru či subjektu údajů) a ve jmenování pověřence na ochranu osobních údajů. Všechny tyto nové povinnosti vycházejí z možného (vysokého) rizika pro práva a svobody subjektů údajů v digitálním prostředí. Předpokladem zákonného fungování subjektů, které se zabývají zpracováním a spravováním osobních údajů (tedy správce[61] a zpracovatele[62]), je tyto povinnosti znát a rovněž mít povědomí o tom, jakým způsobem je naplňovat. Důležité je si uvědomit, že **povinovány nebudou pouze subjekty evropské**. GDPR totiž bude aplikováno v souvislosti se sub-

58 Pokyny k právu na přenositelnost údajů (dokument WP 242, ze dne 13. 12. 2016), otázky a odpovědi, neoficiální překlad z anglického jazyka dostupný na: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=22210.

59 Viz čl. 21 odst. 2 GDPR.

60 Viz čl. 6 odst. 1 písm. e) a f) GDPR.

61 Definice správce viz čl. 4 odst. 7 GDPR.

62 Definice zpracovatele viz čl. 4 odst. 8 GDPR.

jekty osobních údajů, které se nacházejí na území Evropské unie.[63] Umístění sídla či provozovny správce či zpracovatele osobních údajů v tomto případě nebude hrát roli. Jakmile správce nebo zpracovatel bude nakládat[64] s osobními údaji subjektů, které se nacházejí na území EU, musí být připraven splnit veškeré požadavky, které na zpracování osobních údajů klade GDPR.[65]

Již bylo zmíněno, že jedním ze základních požadavků GDPR je odpovědnost správce,[66] jejímž obsahem je **povinnost zavedení, revidování a případné aktualizování vhodných technických a organizačních opatření, aby správce osobních údajů zajistil a také byl schopen doložit zpracování osobních údajů v souladu s GDPR**. Očekává se, že osobní údaje budou zpracovávány pouze pro konkrétní účel, v nezbytném rozsahu, pouze po nutnou dobu (minimalizace) a všude, kde to bude možné, aby byly osobní údaje pseudonymizovány, tj. aby bez dodatečných (odděleně uchovávaných) informací nemohly být přiřazeny konkrétnímu subjektu údajů.[67] **S odpovědností zpracovatele a správce úzce souvisí zajištění příslušné úrovně zabezpečení zpracování osobních údajů zohledňující rizika zničení, pozměnění, neoprávněného zpřístupnění osobních údajů** apod.[68] Pokud dojde k jakémukoliv porušení zabezpečení osobních údajů, je povinností správce bez zbytečného odkladu[69] takovou skutečnost ohlásit dozorovému úřadu a za určitých podmínek i dotčeným subjektům údajů.[70]

Pověřenec pro ochranu osobních údajů[71]

Samostatnou a velmi diskutovanou kapitolou nové úpravy ochrany osobních údajů je osoba pověřence pro ochranu osobních údajů,[72] který **má být ustanoven, aby v příslušné organizaci napomáhal zajišťovat soulad s ustanoveními GDPR**.[73] Jeho jmenování ale není povinné paušálně pro všechny správce či zpracovatele.[74]

Funkce pověřence je **nezbytná tam, kde zpracování provádí orgán veřejné moci nebo veřejný subjekt**,[75] **hlavní činnost správce nebo zpracovatele spočívá v operacích vyžadujících rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo kde hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů**, jako je rasový a etnický původ, politické názory, náboženské vyznání nebo filozofické přesvědčení, členství v odborech, genetické a biometrické údaje nebo údaje o zdravotním stavu nebo sexuálním životě či sexuální orientaci fyzické osoby,[76] a též údajů týkajících se rozsudků v trestních věcech a trestných činů anebo souvisejících bezpečnostních opatření.[77] To znamená, že pokud **činností správce není rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo rozsáhlé zpracování zvláštních kategorií údajů (např. údaje o rasovém původu, genetické nebo biometrické údaje nebo údaje o zdravotním stavu), pak pověřence jmenovat nemusí. Pokud tedy lékař zpracovává osobní údaje svých pacientů, pakliže nejde o zpracování rozsáhlé, rovněž nemusí jmenovat pověřence, i když zpracovává zvláštní kategorii údajů**. Kromě těchto situací může národní právo členských států požadovat jmenování pověřence i v dalších případech. Tak je tomu např. v Německu, které si tuto možnost prosadilo v rámci přípravy GDPR.

Tím není vyloučeno dobrovolné jmenování pověřence pro ochranu osobních údajů v podniku. I dobrovolně jmenovaný pověřenec pro ochranu osobních údajů musí být do funkce ustanoven a svou činnost vykonávat zcela v souladu s veškerými podmínkami GDPR.

Od osoby pověřence je nutné důsledně[78] **odlišovat zaměstnance, který má v podniku v popisu práce zabezpečení řádného zpracování osobních údajů.** Kterýkoliv podnik může ustanovit někoho ze zaměstnanců, aby byl zodpovědný za agendu zpracování osobních údajů, jde však pouze o interní organizační řád podniku a navenek taková osoba nemá postavení pověřence pro ochranu osobních údajů. Jmenování pověřence pro ochranu osobních údajů (ani osoby zodpovědné za zpracování osobních údajů v podniku mimo rámec GDPR) nevylučuje zodpovědnost jednotlivých manažerů za legální zpracování osobních údajů na jejich úseku (např. v personálním oddělení za zpracování osobních údajů zaměstnanců, v obchodním oddělení za zpracování osobních údajů dodavatelů či zákazníků, v IT oddělení za bezpečnost uložených a zpracovávaných osobních údajů) ani vyvinění organizace jako takové z odpovědnosti za řádné zpracování osobních údajů. WP29 v této souvislosti zdůrazňuje,[79] že **pověřenec nenese osobní zodpovědnost za dodržování GDPR, vždy jsou to správci nebo zpracovatelé**, kteří musí shodu zpracování osobních údajů s GDPR zajistit a také ji doložit. Zároveň správce nebo zpracovatel mají důležitou

63 To koresponduje s výkladem učiněným v souvislosti s věcí C-131/12.

64 Podle GDPR jde o činnosti správce nebo zpracovatele, které souvisejí s nabídkou zboží a služeb subjektům údajů v EU (bez ohledu na to, zda jde o zboží a služby zpoplatněné či nikoliv) nebo s monitorováním chování těchto subjektů v rámci EU (viz ust. čl. 3 GDPR).

65 Viz ust. čl. 3 GDPR věnované místní působnosti nařízení.

66 Viz čl 24 GDPR.

67 Viz čl. 4 odst. 5 GDPR.

68 Čl. 32 GDPR.

69 Pokud možno do 72 hodin od okamžiku, kdy se správce o porušení zabezpečení osobních údajů dozvěděl. S pozdějším ohlášením musí být současně poskytnuty dozorovému úřadu také důvody zpoždění.

70 Čl. 33 GDPR.

71 Označovaný též jako DPO – Data Protection Officer.

72 Čl. 37 odst. 1 písm a) až c) GDPR.

73 Konkrétní úkoly pověřence pro ochranu osobních údajů stanoví čl. 39 GDPR a zahrnuje poskytování informací a konzultací, monitoring shody s pravidly GDPR a souvisejícími předpisy na ochranu osobních údajů, spolupráci s dozorovým úřadem vč. toho, že pověřenec je kontaktním místem úřadu.

74 Podmínky (povinného) jmenování pověřence pro ochranu osobních údajů jsou obsaženy v čl. 37 GDPR.

75 S výjimkou soudů jednajících v rámci svých soudních pravomocí [čl. 37 odst. 1 písm. a) GDPR].

76 Údaje obsažené v čl. 9 GDPR.

77 Viz čl. 10 GDPR.

78 Včetně názvu takové funkce či pozice, který by neměl znít „pověřenec pro ochranu osobních údajů“ nebo „DPO“ nebo „Data Protection Officer“, ale např. „manažer pro správu a evidenci osobních údajů“.

79 Na konci loňského roku WP29 publikovala dokument „Vodítka k pověřencům pro ochranu osobních údajů“; schválen dne 13. 12. 2016 a ve znění revize schválené dne 5. 4. 2017 (WP 243 rev. 01) je prostřednictvím internetových stránek ÚOOÚ dostupný na: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23462. V českém překladu ÚOOÚ tento dokument zpřístupňuje na: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23463. V něm jsou obsažena doporučení a názory pracovní skupiny k DPO.

roli ve vytváření podmínek pro účinné plnění úkolů pověřence, zejména mu garantovat dostatečnou samostatnost a zajistit potřebné zdroje[80] pro efektivní výkon jeho funkce.

Jestliže správce nebo zpracovatel má zákonnou povinnost jmenovat pověřence pro ochranu osobních údajů, pak též musí zveřejnit kontaktní údaje pověřence pro ochranu osobních údajů a sdělit je také dozorovému úřadu. Pro zveřejnění není předepsaná žádná forma. To znamená, že podnik může tuto osobu uvést např. na svých webových stránkách, dále pak její jméno a kontakt na ni uvádět zejména v souhlasu se zpracováním osobních údajů, v informacích o zpracování osobních údajů povinně sdělovaným subjektům údajů, v textu věnujícím se cookies[81] zveřejňovaném prostřednictvím webových stránek správce nebo zpracovatele a v interních směrnicích věnovaných ochraně osobních údajů.

Správce či zpracovatel musí pověřence pro ochranu osobních údajů vybrat a jmenovat na základě jeho profesních kvalit, zejména s ohledem na jeho odborné znalosti práva a praxe v oblasti ochrany údajů a schopnosti plnit úkoly stanovené v GDPR, zejména poskytovat poradenství správcům či zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle GDPR a dalších právních předpisech na ochranu osobních údajů; monitorovat plnění povinností podle právních předpisů na ochranu osobních údajů v podniku při zpracování osobních údajů; a poskytovat poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů. Potřebná úroveň odborných znalostí by se měla určit zejména podle prováděných operací zpracování a podle ochrany, která se vyžaduje pro osobní údaje zpracovávané správcem nebo zpracovatelem.[82] **Požadavek GDPR na to, aby pověřenec měl odborné znalosti práva v oblasti ochrany osobních údajů, neznamená, že pověřencem může být pouze kvalifikovaný právník. Jde o osobu, která by měla dobře rozumět vnitřním procesům konkrétního podniku.** V případě rozsáhlého automatizovaného zpracování osobních údajů (což se u profilingu předpokládá) by vhodným pověřencem mohla být např. osoba, která má znalosti v oblasti analýzy dat a kybernetické bezpečnosti.

Ve svých oficiálních praktických doporučeních a výkladových stanoviscích k ustanovením GDPR ohledně funkce pověřence se WP29 poměrně intenzivně věnuje podmínkám jmenování pověřence. Nalezneme zde výklad pojmu „hlavní činnost“, který v souvislosti s podmínkami povinného jmenování pověřence GDPR užívá. WP29 odkazuje na čl. 97 recitálu GDPR, ve kterém je stanoveno, že hlavní činnosti správce souvisejí s jeho činnostmi základními a nevztahují se na zpracování osobních údajů jakožto činnost pomocnou. Zároveň však WP29 také upozorňuje, že nelze vylučovat aktivity, při kterých zpracování dat tvoří nedílnou součást činnosti správce (zpracovatele) údajů. Jako názorný příklad WP29 uvádí nemocnici, jejíž hlavní činností je poskytovat zdravotní péči, což ale není dost dobře možné bez zpracování osobních údajů pacientů (jejich zdravotních záznamů). A to je důvod, proč **v případě nemocnice je zpracování osobních údajů považováno také za hlavní činnost, a tudíž nemocnice je povinna pověřence jmenovat**.

Další pomocný výklad WP29 k podmínkám jmenování pověřence je s odkazem na čl. 91 recitálu GDPR zaměřen na **pojem „rozsáhlé zpracování“**. Výklad nedefinuje hranici, od které lze zpracování považovat za rozsáhlé, i když v souvislosti s praktickou aplikací GDPR se výhledově počítá se vznikem standardního postupu, jak určit, co znamená „rozsáhlý“ ve vztahu k určitým typům zpracování. V tuto chvíli výklad WP29 poskytuje výchozí faktory (jako je počet dotčených subjektů, objem zpracovávaných dat či rozsah datových položek, doba trvání nebo nepřetržitost zpracovatelské činnosti a její územní rozsah), jejichž vyhodnocení napomůže při rozhodování, zda je správce povinen jmenovat pověřence z důvodu rozsáhlého zpracování osobních údajů.

Dále se WP29 vypořádává také s termínem **„pravidelné a systematické monitorování subjektů údajů“** s tím, že pod monitoring je třeba zahrnout všechny formy sledování a profilování[83] na internetu, přičemž ale o pojmu monitorování nelze uvažovat omezeně pouze pro online prostředí. Příkladem činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů podle WP29 je provozování telekomunikačních sítí nebo poskytování telekomunikačních služeb, daty řízený marketing, profilování a skoring pro účely posouzení rizik, např. pro účely hodnocení úvěrového rizika, behaviorální reklama, věrnostní programy, kamerové systémy, inteligentní domy atd.

Slovo **„pravidelný“** WP29 charakterizuje pomocí jedné či kombinací těchto charakteristik: průběžný nebo opakující se v pravidelných intervalech a po určitou dobu; stále se opakující nebo opakovaný v daných časech; neustále nebo pravidelně se vyskytující. Podobným způsobem WP29 vykládá také slovo **„systematický“** jako kombinaci následujících charakteristik: vyskytující se podle určitého systému; přednastavený, organizovaný nebo metodický; uskutečňovaný jako součást obecného plánu pro sběr dat a vykonávaný jako prvek strategie.

Čl. 37 odst. 2 GDPR **umožňuje skupině podniků jmenovat jediného společného pověřence**. To lze ale pouze v případě, že bude snadno dosažitelný z každého jednotlivého podniku. Také v této záležitosti podává WP29 svůj výklad. Pojem **„dosažitelnost“** se vztahuje k pověřenci jako ke kontaktní osobě, a to pro subjekty údajů,[84] dozorové orgány[85] i uvnitř organizace (pro správce nebo zpracovatele a jeho zaměstnance).[86] Aby byla dostupnost zajištěna, musí být k dispo-

80 Např. aktivní podpora od vyššího vedení, dostatečný čas pro plnění povinností, finanční zdroje, nezbytný přístup do jiných útvarů v organizaci – personální, IT aj., průběžná školení atd.

81 Cookies jsou malé textové soubory ukládané na váš počítač v okamžiku, kdy navštívíte nějakou webovou stránku. Mohou být využity k zapamatování uživatelských informací, zaznamenání položek v nákupním košíku a odhalování toho, jak daná osoba využívá síť. Některé cookies, tzv. cookies třetí strany, mohou být také používány pro řadu účelů, včetně zaznamenávání informací o tom, jak uživatel interaguje s dalšími webovými stránkami (definice převzatá z https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=14302&n=tiskova-zprava-wp29-k-pruzkumu-cookies).

82 K úrovni odborných znalostí, profesním kvalitám a schopnostem plnit úkoly se v tomto duchu vyjadřuje také WP29.

83 Definice profilování jako jakékoliv formy automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě... viz čl. 4 odst. 4 GDPR.

84 Čl. 38 odst. 4 GDPR.

85 Čl. 39 odst. 1 písm. e) GDPR.

86 Čl. 39 odst. 1 písm. a) GDPR.

zici kontaktní údaje pověřence a pověřenec musí být schopen účinně komunikovat se subjekty údajů a spolupracovat s dozorovým úřadem. Dosažitelnost pověřence musí být reálná, proto WP29 jako obecné pravidlo doporučuje, aby pověřenec sídlil v EU, a to bez ohledu na skutečné sídlo správce nebo zpracovatele.

Ohlašování případů porušení zabezpečení osobních údajů

Článek 33 GDPR zakotvuje povinnost správce hlásit bez zbytečného odkladu (do 72 hodin od zjištění) dozorovému úřadu jakékoliv porušení zabezpečení osobních údajů. Pokud dojde k prodlevě, poskytne spolu s hlášením dozorovému úřadu také informace o důvodech tohoto zpoždění. Pokud je pravděpodobné, že následkem porušení zabezpečení osobních údajů je vysoké riziko pro práva a svobody subjektů údajů, má správce oznamovací povinnost také vůči těmto subjektům (viz čl. 34 GDPR).

Rezortní kodexy správné praxe

Ke splnění povinností správce osobních údajů dle GDPR budou moci podniky doložit, že zpracování osobních údajů provádějí v souladu se schválenými rezortními kodexy.[87] **GDPR předpokládá, že různé zájmové organizace v jednotlivých sektorech průmyslu vypracují zásady správné praxe**, které budou aplikovat obecné zásady GDPR na konkrétní obor, a tyto poté, co budou schváleny příslušným dozorovým orgánem, budou sloužit jako etalon správné praxe v daném oboru. Akreditované subjekty budou moci o tom vydávat i osvědčení.

Záznamy správce

Za účelem doložení respektování povinností stanovených GDPR budou správci i zpracovatelé povinni vést podrobné záznamy (vedené dle čl. 30 GDPR) o činnostech zpracování. Tyto záznamy lze považovat za určitou náhradu oznamovací povinnosti, kterou GDPR zrušilo.[88]

Vedle záznamů dle čl. 30 GDPR bude třeba, aby podniky měly vytvořeny vnitřní předpisy ohledně zpracování osobních údajů, zavedeny mechanismy pro posuzování vlivu činnosti podniku na ochranu osobních údajů,[89] a to zejména u druhů zpracování, která mohou znamenat vysoké riziko pro práva a svobody fyzických osob (vč. případné předchozí konzultace s relevantním dozorovým úřadem podle čl. 36 GDPR), či spolupráci (na žádost) s příslušným dozorovým úřadem.[90]

87 Čl. 40 a násl. GDPR.
88 Výjimka z povinnosti vést záznamy viz čl. 30 odst. 5 GDPR.
89 Podle čl. 35 GDPR.
90 Čl. 31 GDPR.

Postihy za nedodržení pravidel GDPR

Vedle možnosti soudní i mimosoudní ochrany v případě porušení práv při zpracovávání osobních údajů tak definuje GDPR v čl. 83 podmínky pro ukládání správních pokut. V tisku se často zmiňují vysoké horní hranice pokut, které GDPR umožňuje uložit v případě nedodržování pravidel pro zpracování osobních údajů. **Maximální výše pokuty je stanovena ve výši 20 milionů eur nebo, jedná-li se o podnik, až do výše 4 % z celkového ročního obratu celosvětově za předchozí finanční rok** (záleží, která z hodnot je vyšší).

U každého individuálního případu je nutné zajistit účinnost a přiměřenost sankce, aby uložená pokuta měla odrazující funkci. Otázkou stále zůstává, jak bude možné dosáhnout harmonizace výše pokut na území EU v situaci, kdy jsou ekonomiky členských států stále velmi odlišné.

V tomto okamžiku samozřejmě nelze predikovat, jak budou dozorové úřady postupovat při ukládání pokut v konkrétních případech. To ukáže až praxe.

Je pesimismus namístě?

Jak se blíží nástup účinnosti GDPR, množí se obavy a dotazy na složitost naplnění požadavků GDPR. Nabízí se však také jiný přístup. Dívat se na GDPR jako na příležitost, jako na možnost nastolit ve firmě pořádek v oblasti ochrany osobních údajů a nakládání s nimi. Možným východiskem je datový audit, po kterém pak bude následovat implementace jednotlivých opatření k zajištění shody s GDPR. Zásadní investice předpokládáme zejména u podniků, které se dosud ochranou osobních údajů příliš nezabývaly, a u správců provádějících rozsáhlé automatizované zpracování osobních údajů, zejména v oblasti monitorování subjektů údajů a predikce jejich chování v prostředí internetu a internetové reklamy. Jako velmi pozitivní vnímáme možnost vzniku profesních kodexů správné praxe, které umožní zohlednit specifika v různých podnikatelských oborech a mohou přinést právní jistotu do podnikání. Vznik takových profesních kodexů však bude jistě nějakou dobu trvat, navíc je žádoucí, aby tyto kodexy byly harmonizovány napříč členskými státy EU. ✤

Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů

Tento článek se zaměřuje v první řadě na aplikaci obecného nařízení o ochraně osobních údajů v pracovněprávních vztazích a dále pak na souhlas subjektu údajů, který i nadále zůstává jedním ze stěžejních právních titulů pro zákonné zpracování jak osobních údajů, tak zvláštních kategorií osobních údajů. Pozornost je dále věnována právům zaměstnance jakožto subjektu údajů a také administrativním povinnostem správce, které se rozšířily a budou se samozřejmě dotýkat rovněž zaměstnavatelů. V neposlední řadě je popsán nový institut, kterým je pověřenec pro ochranu osobních údajů, s nímž je spojena řada pracovněprávních konsekvencí. Závěrem jsou nastíněny právní prostředky ochrany, které GDPR upravuje.

Mgr. Hana Zemanová Šimonová, LL.M.,

je partnerkou AK Bulinský, Vávra & Partners, advokátní kancelář, s. r. o., a doktorandkou na PF MU v Brně.

Reforma ochrany osobních údajů v EU byla definitivně schválena v dubnu 2016 a její vlajkovou lodí je nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) (dále jen „obecné nařízení" nebo také „GDPR"), kterým se ruší dosavadní směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice"). Předmětné obecné nařízení nabude účinnosti dne 25. 5. 2018.

Ačkoliv bývá, zejména pak v médiích, nová koncepce ochrany osobních údajů v EU prezentována jako bezmála revoluční, je třeba podotknout, že obecné nařízení se od směrnice nikterak nedistancuje, ale naopak výslovně stanoví, že cíle a zásady směrnice nadále platí.[1] Spíše než o revoluční změně je proto vhodné hovořit o kontinuitě právní úpravy.[2] Obecné nařízení bylo přijato zejména za účelem sjednocení roztříštěné právní úpravy vzniklé v důsledku nejednotné implementace směrnice do právních řádů členských států a rozličných postupů jednotlivých dozorových úřadů.

Sluší se podotknout, že řada základních pojmů spojených s právem na ochranu osobních údajů je jak ve směrnici, tak v GDPR vymezena obdobným, často dokonce shodným způsobem.[3] Nicméně, **GDPR samozřejmě přináší celou řadu nových právních institutů i práv a povinností dotčených subjektů, přičemž ty nejvýznamnější z hlediska základních pracovněprávních vztahů budou dále podrobněji analyzovány**. Pozornost bude věnována vybraným institutům GDPR, které mají úzký vztah k základním pracovněprávním vztahům, ať již s ohledem na souvislost s povinnostmi zaměstnavatele jakožto správce, nebo s právy zaměstnance coby subjektu údajů.

Aplikace GDPR v pracovněprávních vztazích

Ačkoliv je cílem GDPR stanovit jednotná práva a povinnosti v oblasti ochrany osobních údajů, mnohá jeho ustanovení buď přímo ukládají členským státům povinnost, nebo jim dávají alespoň možnost upravit na vnitrostátní úrovni vymezenou problematiku samostatně, vždy samozřejmě v souladu se základními zásadami, na nichž je GDPR vystavěno,[4] a v mezích dalších limitů předepsaných GDPR. Pro pracovněprávní problematiku je podstatná např. možnost členských států zavést konkrétnější podmínky zpracování osobních údajů v případech, kdy je právním titulem pro zpracování osobních údajů plnění právní povinnosti správce.[5]

Současně je nutné se blíže věnovat ustanovení **čl. 88 GDPR**, které členským státům umožňuje buď právním předpisem, anebo kolektivní smlouvou ***„stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, plnění pracovní smlouvy, včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuál-***

1 Viz bod odůvodnění (9) GDPR.

2 Kupř. stávající pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená dle čl. 29 směrnice (dále jen „Pracovní skupina") již nyní vydává metodické pokyny a vodítka týkající se GDPR (viz níže), přičemž po nabytí účinnosti GDPR bude transformována na Evropský sbor pro ochranu osobních údajů, viz čl. 68 a násl. GDPR.

3 Důkazem nechť jsou prakticky shodné, popř. jen drobně a nikoliv významově podstatně upravené definice základních pojmů práva na ochranu osobních údajů, a to včetně samotného pojmu „osobní údaj", „zpracování", „správce", „zpracovatel". K tomu viz Úřad pro ochranu osobních údajů, Desatero omylů o obecném nařízení (GDPR) [online], 2017, 5 stran. [cit. 22. 6. 2017]. A dále k tomu viz M. Nulíček a kol.: GDPR, Obecné nařízení o ochraně osobních údajů, Praktický komentář, 1. vydání, Wolters Kluwer ČR, Praha 2017, str. 73 a násl.

4 Viz zejména čl. 5 GDPR.

5 Viz čl. 6 odst. 2 GDPR.

ního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru".[6]

Pravidla přijatá členskými státy na podkladě výše uvedeného oprávnění dle čl. 88 GDPR však musejí zahrnovat zvláštní a vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, především pokud jde o transparentnost zpracování, předávání osobních údajů v rámci skupiny podniků a systémy monitorování na pracovišti.[7] Stejně tak bude nezbytné, aby tato pravidla vycházela ze zásad, na nichž je nová koncepce ochrany osobních údajů vystavěna.[8] Ve smyslu ust. čl. 88 odst. 3 GDPR mají členské státy notifikační povinnost vůči Komisi, kdy jsou povinny nejpozději do 25. 5. 2018 oznámit Komisi právní předpisy přijaté dle předmětného ustanovení, stejně jako jsou povinny bez zbytečného odkladu informovat Komisi o jakýchkoliv následných změnách takto přijatých právních předpisů.

Lze tedy konstatovat, že **i v rámci pracovněprávních vztahů bude třeba respektovat GDPR a řídit se jeho ustanoveními, nicméně, pokud bude členským státem přijata speciální právní úprava** v mezích stanovených mj. čl. 88 GDPR, což bude spíše pravidlem, např. pokud jde o podmínky pro zpracování osobních údajů na základě souhlasu zaměstnance nebo podmínky pro monitorování pracoviště, **vztah mezi GDPR a přijatou či existující vnitrostátní právní úpravou bude vztahem obecného a speciálního právního předpisu**, kdy v souladu s obecnou zásadou *lex specialis derogat legi generali* bude aplikován speciální právní předpis upravující konkrétnější podmínky pro zpracování osobních údajů. Nutno podotknout, že v tomto směru nedochází k žádné podstatné změně oproti nynějšímu stavu fungujícímu na bázi směrnice a na základě ní přijatých právních předpisů členských států.

Souhlas se zpracováním osobních údajů

Souhlas i nadále zůstává jedním z důvodů pro zákonné zpracování osobních údajů, ovšem **podmínky získávání souhlasu subjektu údajů se zpracováním osobních údajů a prokazování jeho existence jsou oproti nynější právní úpravě znatelně přísnější**. Souhlasem se dle obecného nařízení rozumí *„jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů"*.[9] Souhlas může být udělen jak písemným prohlášením, tak elektronicky nebo ústně, ovšem musí se jednat o jednoznačné potvrzení, přičemž za souhlas nelze považovat zejména mlčení, předem zaškrtnuté políčko nebo nečinnost subjektu údajů.[10]

Podmínky vyjádření souhlasu blíže upravuje ust. čl. 7 GDPR, v jehož odst. 1 je stanoveno, že **správce je povinen prokázat, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů**. Vzhledem k tomuto požadavku lze dovodit, že ústně vyjádřený souhlas subjektu údajů, byť ústní forma souhlasu je GDPR výslovně připuštěna,[11] nebude prakticky realizovatelný, neboť správce by v takovém případě nemohl dostát své povinnosti doložit udělení souhlasu se zpracováním osobních údajů ze strany subjektu údajů. Ze stejného důvodu lze mít pochybnosti o tom, že bude v praxi častý konkludentní souhlas subjektu údajů se zpracováním osobních údajů.[12]

V případě, kdy je souhlas vyjádřen písemným prohlášením,[13] vyžaduje ust. čl. 7 odst. 2 GDPR, **aby souhlas se zpracováním osobních údajů byl od jiných ustanovení podepisovaného dokumentu jasně odlišitelný, srozumitelný a snadno přístupný a aby byl formulován za použití jasných a jednoduchých jazykových prostředků a prostý nepřiměřených podmínek**.[14] Porušení tohoto požadavku je sankcionováno nezávazností uděleného souhlasu. Z uvedeného důvodu **by měl být souhlas obsažen v samostatném, jasně a srozumitelně koncipovaném dokumentu**, obsahujícím mj. informace dle čl. 12 a násl. GDPR.[15]

Z pohledu základních pracovněprávních vztahů, jejichž charakteristickým znakem je vztah nadřízenosti zaměstnavatele a podřízenosti zaměstnance, je třeba upozornit na **bod odůvodnění (42) GDPR, dle něhož nebude souhlas považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout, aniž by byl poškozen**. Uvedené ustanovení však nikterak nepřibližuje, o jaký druh poškození, popř. jaké intenzity, se má jednat. Za situace, kdy je kupř. po zaměstnanci požadováno, aby udělil souhlas s vystavením své fotografie na webových stránkách zaměstnavatele, si lze představit, že neudělení tohoto souhlasu by pro daného zaměstnance mohlo představovat negativní situaci v zaměstnání, ať již se jedná o „pouhé" zhoršení mezilidských vztahů na pracovišti, nebo zpomalení kariérního růstu, nepřiznání pohyblivé složky mzdy apod.

V této souvislosti je třeba zdůraznit, že zpracování osobních údajů zaměstnanců, kde právním titulem tohoto zpracování má být souhlas zaměstnance, je třeba vždy posuzovat s ohledem na konkrétní okolnosti případu, přičemž široké využití souhlasu jakožto právního titulu zpracování osobních údajů nelze v základních pracovněprávních vztazích v žádném případě doporučit. Při posuzování platnosti udělení souhlasu je třeba aplikovat princip proporcionality a zvážit, nakolik je právo na ochranu osobních údajů zaměstnance v rovnováze s oprávněnými zájmy zaměstnavatele, např. pokud jde o jeho zájem o zveřejnění fotografie zaměstnance z důvodu budování firemní kultury a jednotné vizuální stránky webové prezentace.[16]

6 Viz čl. 88 odst. 1 GDPR. K tomu srov. bod odůvodnění (155) GDPR.
7 Viz čl. 88 odst. 2 GDPR.
8 Viz především čl. 5 GDPR.
9 Viz čl. 4 odst. 11 GDPR.
10 Viz bod odůvodnění (32) GDPR.
11 Tamtéž.
12 K tomu srov. M. Nulíček a kol., op. cit. sub 3, str. 147-148.
13 Včetně elektronické formy, viz tamtéž, str. 150.
14 Viz také bod odůvodnění (42) GDPR.
15 V souvislosti se souhlasy udělenými dle směrnice, resp. ZOOÚ, je však třeba upozornit, že *„není nutné, aby subjekt údajů znovu udělil svůj souhlas, pokud je způsob udělení daného souhlasu v souladu s podmínkami tohoto nařízení..."*, viz bod odůvodnění (171) GDPR. V každém případě však bude nezbytné podrobit doposud udělené souhlasy důkladnému přezkoumání a popř. zajistit souhlasy subjektů údajů v takové podobě a formě, aby odpovídaly právní úpravě obsažené v GDPR, zejména pak, aby správce dostál své povinnosti existenci souhlasu subjektu údajů doložit.
16 V této souvislosti je vhodné poukázat na bod odůvodnění (47) GDPR, který říká, že *„oprávněné zájmy správce, včetně správce, jemuž mohou být osobní údaje poskytnuty, nebo třetí strany, se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem. ... Oprávněným zájmem dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům..."*.

Ještě závažněji se z pohledu pracovněprávních vztahů jeví ustanovení **bodu odůvodnění (43) GDPR, dle něhož by vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů v případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha**. V oblasti základních pracovněprávních vztahů, jejichž objektem je závislá práce a které jsou ze samotné své podstaty fakticky nerovné a postavené na tom, že zaměstnavatel vystupuje jako řídící subjekt a zaměstnanec je subjektem podřízeným, si lze však při extenzivním výkladu představit, že by souhlas jako zákonný titul pro zpracování údajů zaměstnavatelem nemohl být platně udělen prakticky za žádné situace, což zřejmě nebylo úmyslem zákonodárce. Nejen v intencích doporučení Pracovní skupiny[17] **je však třeba souhlas zaměstnance jakožto právní titul ke zpracování osobních údajů využívat obezřetně a spíše jen sporadicky**, při vědomí specifik základních pracovněprávních vztahů a v rámci nich působící ochranné funkce pracovního práva a z ní vyplývající zásady zvláštní zákonné ochrany postavení zaměstnance.[18] Pokud již bude souhlas zaměstnance využit jako právní titul ke zpracování jeho osobních údajů, pak je doporučeníhodné trvat na tom, aby po předchozím důsledném zvážení všech konkrétních okolností a využití principu proporcionality byla zvolena písemná forma souhlasu.

Oproti stávající právní úpravě obsažené ve směrnici a ZOOÚ se v GDPR výslovně stanoví, že **subjekt údajů má právo svůj souhlas kdykoliv odvolat, přičemž odvolání souhlasu musí být stejně jednoduché jako jeho poskytnutí**.[19] S ohledem na explicitní vyjádření odvolání souhlasu, které však bylo Pracovní skupinou deklarováno již za nynější právní úpravy,[20] zřejmě pozbyly smyslu úvahy o aplikovatelnosti ust. § 87 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „o. z."), a o případném nároku na náhradu škody způsobené správci v důsledku odvolání souhlasu na dobu určitou, neboť ust. čl. 7 odst. 3 GDPR je speciálním ve vztahu k § 87 odst. 2 o. z.

Výslovný souhlas se zpracováním zvláštních kategorií osobních údajů

Dle ust. čl. 9 odst. 1 GDPR 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"*.[21] Obecné nařízení používá pro shora vyjmenované osobní údaje označení ***„zvláštní kategorie osobních údajů"***, a nikoliv dosud používané *„citlivé údaje"*, ovšem nejen v rámci českého právního prostředí lze očekávat, že zažitý pojem *„citlivé údaje"* bude používán i nadále.[22]

Zákaz uvedený v čl. 9 odst. 1 GDPR se neuplatní v případech vyjmenovaných v čl. 9 odst. 2 GDPR, přičemž **jedním z právních titulů pro zákonné zpracování zvláštních kategorií osobních údajů je výslovný souhlas subjektu údajů**. K tomuto bodu je vhodné uvést dvě poznámky.

- Prvně je nutné se blíže věnovat **požadavku na existenci výslovného souhlasu**. Kromě podmínek stanovených obecným nařízením pro „prostý" souhlas subjektu údajů se zpracováním osobních údajů, o nichž bylo pojednáno v podrobnostech výše, musí být souhlas se zpracováním zvláštních kategorií osobních údajů výslovný. Je tedy vyloučen, stejně jako za nynější právní úpravy, konkludentní souhlas se zpracováním zvláštních kategorií osobních údajů, neboť je vyžadováno explicitní vyjádření souhlasu subjektu údajů. Vzhledem k přísnějším požadavkům na projev „prostého" souhlasu subjektu údajů se zpracováním osobních údajů a s ohledem na povinnost správce být schopen existenci souhlasu kdykoliv doložit, lze konstatovat, že se rozdíl mezi „prostým" souhlasem a „výslovným" souhlasem poněkud stírá. **Pro základní pracovněprávní vztahy lze poznamenat, že pokud je souhlas zaměstnance jako právní titul ke zpracování osobních údajů institutem, který je třeba z důvodů uvedených výše využívat pokud možno co nejméně, zpracování zvláštních kategorií osobních údajů zaměstnanců na základě jejich výslovného souhlasu bude spíše výjimečné.**
- Za druhé je vhodné upozornit, že členským státům, stejně jako EU samotné, bylo ustanovením čl. 9 odst. 2 písm. a) GDPR umožněno, aby právním předpisem vyloučily zpracování určitých zvláštních kategorií osobních údajů na základě souhlasu subjektu údajů, byť výslovně projeveného. V souvislosti se základními pracovněprávními vztahy se tak samozřejmě i nadále uplatní ust. § 316 odst. 4 zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „zák. práce"), které vyjmenovává informace, resp. citlivé údaje, které zaměstnavatel po zaměstnanci nesmí vyžadovat za žádných okolností, a tedy ani v případě eventuálního výslovného souhlasu zaměstnance.[23]

Vybraná práva subjektu údajů dle GDPR

Práva subjektů údajů, která samozřejmě přísluší rovněž zaměstnanci jakožto subjektu údajů, jsou v GDPR oproti stávající právní úpravě obsažené zejména v ust. § 21 ZOOÚ

17 Viz Article 29 – Data Protection Working Party, Opinion 2/2017 on data processing at work, WP 249 [online], Brussel: European Commission, 2017, str. 6 [cit. 29. 6. 2017]. Dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

18 Srov. M. Nulíček a kol., op. cit. sub 3, str. 145 a násl.

19 Viz čl. 7 odst. 3 GDPR.

20 Viz Article 29 – Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, WP 48 [online], Brussel: European Commission, 2001, str. 23 [cit. 5. 6. 2017]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf.

21 Viz čl. 9 odst. 1 GDPR. Z citovaného znění je zřejmé, že mezi zvláštní kategorie osobních údajů nejsou nově řazeny osobní údaje vypovídající o odsouzení za trestný čin, jimž je věnováno speciální ust. čl. 10 GDPR a které nově představují zvláštní kategorii osobních údajů, jejichž zpracování je možné za přísných podmínek uvedených v tomto ustanovení.

22 O tom svědčí i terminologie použitá v komentáři, viz M. Nulíček a kol., op. cit. sub 3, str. 162 a násl. Rovněž lze poukázat na bod odůvodnění (51) GDPR, kde se hovoří o osobních údajích, *„které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod…"*.

23 Dle ust. § 316 odst. 4 zák. práce nesmí zaměstnavatel od zaměstnance ani prostřednictvím třetích osob vyžadovat či získávat informace, které bezprostředně nesouvisejí s výkonem práce a se základním pracovněprávním vztahem, zejména pak nesmí vyžadovat informace o těhotenství, rodinných a majetkových poměrech, sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnosti k církvi nebo náboženské společnosti nebo trestněprávní bezúhonnosti. Jestliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, příp. pokud tak stanoví zák. práce nebo jiný právní předpis, je možné po zaměstnanci vyžadovat i výše uvedené informace, s výjimkou informace o sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnosti k církvi nebo náboženské společnosti, když vyžadování nebo zjišťování těchto informací je vyloučeno za všech okolností.

upravena podrobněji, některá dokonce zcela nově, jak bude demonstrováno v následujícím výkladu.

Na základě čl. 15 GDPR má subjekt údajů právo požadovat po správci jednak potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud ano, pak má právo na přístup k osobním údajům a k informacím vyjmenovaným v čl. 15 odst. 1 GDPR. Součástí práva na přístup k osobním údajům je oprávnění subjektu údajů požadovat kopii zpracovávaných osobních údajů, přičemž pořízení dalších kopií může být správcem podmíněno uhrazením přiměřeného administrativního poplatku. Současně platí, že právem získat kopii osobních údajů nesmí být nepříznivě dotčena práva a svobody jiných osob.[24] V souvislosti se základními pracovněprávními vztahy je třeba upozornit na ust. § 312 zák. práce, které upravuje vedení osobního spisu zaměstnance a v jehož odst. 3 je zakotveno právo zaměstnance nahlížet do osobního spisu, stejně jako si pořizovat stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele. Vzhledem k tomu, že ust. § 312 zák. práce je ve vztahu k ust. čl. 15 GDPR speciálním ustanovením, uplatní se pravidlo v něm stanovené, a tedy pořizování fotokopií osobních údajů obsažených v osobním spise zaměstnance bude vždy na náklady zaměstnavatele.

Dle ust. čl. 16 GDPR má subjekt údajů právo na opravu nepřesných osobních údajů, které se ho týkají, stejně tak jako má právo na doplnění neúplných osobních údajů, a to s přihlédnutím k účelům zpracování.

V následujícím článku je zakotveno právo subjektu údajů požadovat, aby správce bez zbytečného odkladu vymazal osobní údaje, které se ho týkají,[25] a to za předpokladu, že je dán některý z důvodů uvedených v čl. 17 odst. 1 písm. a) až f) GDPR.[26] V ust. čl. 17 odst. 3 písm. a) až e) GDPR jsou uvedeny případy, kdy se nárok na výmaz neuplatní.[27]

Na základě ust. čl. 18 GDPR má subjekt údajů právo na omezení zpracování,[28] kterým se rozumí označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnosti, přičemž tohoto cíle lze dosáhnout např. dočasným přesunem osobních údajů do jiného systému zpracování nebo znepřístupněním předmětných osobních údajů či dočasným odstraněním osobních údajů z internetových stránek.[29] Právo požadovat omezení zpracování má subjekt údajů toliko v případech uvedených v čl. 18 odst. 1 GDPR,[30] přičemž po dobu omezení zpracování mohou být osobní údaje zpracovány, s výjimkou jejich uložení, pouze se souhlasem subjektu údajů a z důvodů uvedených v čl. 18 odst. 2 GDPR.

Zcela novým právem, které mohou subjekty údajů využít, je **právo na přenositelnost údajů**[31] **dle čl. 20 GDPR**, na základě jehož odst. 1 má subjekt údajů právo *„získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil“*,[32] a to v některém z případů uvedených v tomto ustanovení, mj. za situace, kdy je právním titulem ke zpracování osobních údajů souhlas subjektu údajů.[33]

Je-li právním titulem pro zpracování osobních údajů buď nezbytnost pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, anebo nezbytnost pro účely oprávněných zájmů správce nebo třetí strany, pokud před těmito zájmy nemají přednost zájmy nebo základní práva a svobody subjektu údajů,[34] pak má subjekt údajů právo vznést námitku proti zpracování osobních údajů, a to z důvodů vyplývajících z jeho konkrétní situace.[35] Na právo vznést námitku musí být subjekt údajů výslovně upozorněn *„a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů“*.[36]

V souvislosti s výše uvedenými právy subjektů údajů je třeba upozornit na **povinnost správce poskytnout subjektu údajů na jeho žádost dle čl. 15 až 22 GDPR informace o přijatých opatřeních**, a to bez zbytečného odkladu, nejpozději však do jednoho měsíce od obdržení žádosti. Uvedenou jednoměsíční lhůtu je možné prodloužit toliko z důvodu složitosti věci nebo počtu žádostí, a to o dva měsíce. O tomto prodloužení, stejně jako o jeho důvodech, je správce povinen subjekt údajů informovat. Za situace, kdy správce nepřijme opatření, která subjekt údajů požadoval, je povinen o tomto závěru a důvodech k němu vedoucích subjekt bezodkladně, nejpozději však do jednoho měsíce od přijetí žádosti, informovat a poučit ho o možnosti podat stížnost u dozorového úřadu nebo se domáhat soudní ochrany u příslušného soudu.[37] Na obranu proti zjevně nedůvodným či nepřiměřeným žádostem, zejména z důvodu jejich opakování, je správci umožněno, aby buď subjektu údajů uložil přiměřený poplatek zohledňující administrativní náklady, nebo aby žádosti odmítl vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti je správce povinen v duchu zásady odpovědnosti doložit.[38]

Vybrané povinnosti správce dle GDPR

Obecné nařízení s sebou přináší celou řadu nových, popř. modifikovaných či rozšířených povinností správců, které budou nepochybně znamenat větší administrativní zátěž správců, a tím pádem i zaměstnavatelů.[39]

24 Viz čl. 15 odst. 3 a 4 GDPR.

25 Tzv. *„právo být zapomenut“*.

26 Tímto důvodem je např. skutečnost, že osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny, nebo subjekt údajů odvolá souhlas, na jehož základě byly osobní údaje zpracovány.

27 Např. za situace, kdy je zpracování osobních údajů nezbytné pro účely archivace ve veřejném zájmu.

28 Jedná se do jisté míry o obdobu současné institutu blokování osobních údajů dle § 21 odst. 1 ZOOÚ. K tomu viz M. Nulíček a kol., op. cit. sub 3, str. 215 a násl.

29 Viz čl. 4 odst. 3 ve spojení s bodem odůvodnění (67) GDPR.

30 Např. v případě, kdy subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost údajů prověřit, nebo za situace, kdy subjekt údajů vznesl námitku ve smyslu ust. čl. 21 odst. 1 GDPR.

31 Označováno též jako *„právo na portabilitu“*.

32 Viz čl. 20 odst. 1 GDPR.

33 K tomu více viz M. Nulíček a kol., op. cit. sub 3, str. 221 a násl.

34 Viz čl. 6 odst. 1 písm. e) a f) GDPR.

35 Viz čl. 21 odst. 1 GDPR. Právo vznést námitku má subjekt údajů rovněž proti zpracování osobních údajů pro účely přímého marketingu a pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za podmínek uvedených v čl. 21 odst. 2, 3 a 6 GDPR.

36 Viz čl. 21 odst. 4 GDPR.

37 Viz čl. 12 odst. 3 a 4 GDPR.

38 Viz čl. 12 odst. 5 GDPR.

39 K tomu viz také D. Burian, Z. Radičová: K některým povinnostem, které pro správce přináší obecné nařízení o ochraně osobních údajů (GDPR), Právní prostor [online] 2016 [cit. 10. 7. 2017]. Dostupné z: http://www.pravniprostor.cz/clanky/ostatni-pravo/k-nekterym-povinnostem-ktere-pro-spravce-prinasi-gdpr.

Na prvním místě je vhodné uvést ust. čl. 12 GDPR, kde je zakotvena **povinnost správce mít transparentní, srozumitelná a snadno dostupná pravidla pro zpracování osobních údajů a výkon práv subjektu údajů**. Tato povinnost je evidentním promítnutím zásady transparentnosti a jejím cílem je poskytnout subjektu údajů dostatek informací o tom, jaké údaje a jakým způsobem správce zpracovává. Správce je povinen poskytovat subjektu údajů stanovené informace[40] a veškerá předepsaná sdělení o zpracování[41] stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, přičemž tyto informace mají být poskytnuty písemně nebo jinými prostředky, včetně elektronických prostředků, a pokud si to subjekt údajů vyžádá, lze je poskytnout ústně, je-li identita subjektu údajů prokázána jinými způsoby.[42] Za účelem splnění této informační povinnosti je správce povinen přijmout vhodná, nikoliv však blíže specifikovaná opatření. Bude se zřejmě jednat především o revizi, popř. vytvoření nových podmínek pro zpracování osobních údajů, v nichž budou jasným a srozumitelným způsobem uvedeny všechny informace, upozornění a sdělení tak, jak je GDPR vyžadováno.[43]

S povinnostmi správce a rovněž s ústředním principem odpovědnosti správce, jak ostatně napovídá samotné označení tohoto ustanovení, úzce souvisí čl. 24 GDPR, dle jehož odst. 1 *„s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována."*[44] Z citovaného ustanovení je zřejmé, že povinností správce bude nejprve náležitě posoudit konkrétní a specifické okolnosti zpracování konkrétních osobních údajů a současně zvážit rizika tohoto zpracování pro základní práva a svobody subjektu údajů. V návaznosti na takto provedenou důkladnou analýzu pak správce zavede vhodná technická i organizační opatření, jejichž cílem je zajištění zpracování osobních údajů v souladu s GDPR. Správce je současně povinen doložit soulad zpracování osobních údajů s GDPR, přičemž tento bude dokládán zejména adekvátní dokumentací vyhotovenou pro příslušný účel a vytvořením koncepce na ochranu osobních údajů.[45] Obecné nařízení nepředkládá konkrétní vodítko pro obsah dokumentace, ovšem lze usuzovat na to, že **jejím obsahem by mělo být především vyhodnocení rizik pro základní práva a svobody subjektů údajů, doložení právního titulu pro zpracování osobních údajů, způsob řešení žádostí subjektů údajů k uplatnění jejich práv, konkretizace technických a organizačních opatření sloužících k zajištění souladu zpracování osobních údajů s GDPR atd.**[46]

V souvislosti se zásadou odpovědnosti a požadavkem na doložení souladu postupu správce s GDPR by správce měl *„přijmout vnitřní koncepce a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by mohla mimo jiné spočívat v minimalizaci zpracování osobních údajů, co nejrychlejší pseudonymizaci osobních údajů, transparentnosti s ohledem na funkce a zpracování osobních údajů, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky."*[47] V návaznosti na citované ustanovení bodu odůvodnění (78) je v čl. 25 GDPR upravena *„Záměrná a standardní ochrana osobních údajů"*,[48] která je projevem relativně nového principu *„Privacy by Design"*.[49] **Obecné nařízení tak klade důraz na ochranu osobních údajů, která je již vtělena do technologií a postupů utvářených a zaváděných takovým způsobem, aby pokud možno co nejvíce přispívaly či napomáhaly k ochraně osobních údajů.**

V textu GDPR lze však nalézt celou řadu dalších ustanovení a institutů, z nichž lze dovodit požadavky na vyšší míru odpovědnosti správce a na ni navazující povinnosti správce, a to např. vedení záznamů o činnostech zpracování dle čl. 30 GDPR, které do jisté míry nahrazuje stávající oznamovací povinnost upravenou v § 16 a násl. ZOOÚ.[50]

Velmi administrativně náročné a zřejmě často i fakticky neproveditelné se jeví ohlašování případů porušení zabezpečení osobních údajů dozorovému orgánu, tedy v ČR ÚOOÚ. Dle ust. čl. 33 odst. 1 GDPR je správce povinen ohlásit jakékoliv porušení zabezpečení osobních údajů dozorovému úřadu, a to bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl.[51] V případě, že v této lhůtě není podáno ohlášení, je třeba dozorovému orgánu sdělit důvody nedodržení této lhůty. Ohlašovací povinnost správce nemá za situace, pokud je nepravděpodobné, že by dané porušení mělo za následek riziko pro práva a svobody fyzických osob.

Posouzení existence pravděpodobného vysokého rizika pro práva a svobody fyzických osob je relevantní rovněž pro institut oznamování případů porušení zabezpečení osobních údajů subjektu údajů. Jestliže správce dospěje k závěru, že je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude představovat vysoké riziko pro základní práva a svobody fyzických osob, je povinen toto porušení oznámit subjektu údajů, a to bez zbytečného odkladu a za využití jasných a jednoduchých jazykových prostředků, není-li dán některý z důvodů uvedených v čl. 34 odst. 3 GDPR.[52]

40 Tyto jsou vyjmenovány v čl. 13 a 14 GDPR.

41 Viz čl. 15 až 22 a čl. 34 GDPR.

42 Viz čl. 12 odst. 1 GDPR.

43 K tomu viz M. Nulíček a kol., op. cit. sub 3, str. 177 a násl.

44 Viz čl. 24 odst. 1 GDPR.

45 Viz čl. 24 odst. 2 GDPR. Dle ust. čl. 24 odst. 3 GDPR platí, že *„jedním z prvků, jimiž lze doložit, že správce plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42."*

46 Viz M. Nulíček a kol., op. cit. sub 3, str. 254 a násl.

47 Viz bod odůvodnění (78) GDPR.

48 Jedná se o překlad anglického *„Data protection by design and by default"*.

49 Vznik tohoto přístupu je dáván do souvislosti s kanadskou komisařkou ochrany osobních údajů Ann Cavoukianovou, resp. její knihou *„Privacy by Design"*, přičemž hlavní myšlenkou tohoto přístupu je implementace nástrojů na ochranu soukromí již do návrhů technologií tak, aby se efektivně předcházelo eventuálnímu zneužití zejména osobních údajů. Viz Úřad pro ochranu osobních údajů, Privacy by design, A. Cavoukian. Toronto, Ontario – Canada, 2009 [online], 2013, str. 1–2 [cit. 26. 6. 2017]. Dostupné z: https://www.uoou.cz/privacy-by-design-a-cavoukian-toronto-ontario-canada-2009/ds-2307/p1=2307.

50 Dle čl. 30 odst. 1 GDPR je správce povinen vést záznamy o činnostech zpracování, za které je odpovědný, přičemž tyto záznamy obsahují informace vyjmenované v čl. 30 odst. 1 písm a) až g) GDPR. K podmínkám vedení záznamů o činnostech zpracování viz čl. 30 GDPR.

51 Informace, které musí ohlášení obsahovat, jsou vyjmenovány v čl. 33 odst. 3 GDPR.

52 Viz čl. 34 odst. 1, 2 a 3 GDPR.

Novou povinností uloženou správcům je vyhotovování posouzení vlivu na ochranu osobních údajů, které je třeba před započetím se zpracováním osobních údajů zpracovat, *„pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob“.*[53] Obecné nařízení v čl. 35 odst. 3 obsahuje demonstrativní výčet případů, kdy je nezbytné posouzení vlivu na ochranu osobních údajů zpracovat, a to mj. **v případě systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatickém zpracování, pokud je na něm založeno rozhodování vyvolávající ve vztahu k fyzickým osobám právní účinky nebo jiné závažné dopady**. Za situace, kdy je jmenován pověřenec pro ochranu osobních údajů (viz níže), je správce povinen si vyžádat rovněž jeho posudek.[54] Pracovní skupina již vypracovala vodítka pro zpracování posouzení vlivu na ochranu osobních údajů a pro posouzení otázky, zda zpracování osobních údajů představuje v konkrétním případě vysoké riziko pro základní práva a svobody subjektů údajů.[55] Lze předpokládat, že tato vodítka se stanou cenným podkladem jak pro úvahy správců, zda k vyhotovení posouzení vlivu na ochranu osobních údajů přistoupit, tak pro vlastní zpracování posouzení vlivu na ochranu osobních údajů.

V případě, že posouzení vlivu na ochranu osobních údajů bude ukončeno se závěrem, že by předmětné zpracování osobních údajů mělo, bez přijetí opatření ke zmírnění rizika, za následek vysoké riziko pro základní práva a svobody fyzických osob, **je správce povinen před zahájením zpracování osobních údajů konzultovat danou otázku s dozorovým úřadem** a v této souvislosti sdělit dozorovému úřadu informace uvedené v čl. 36 odst. 3 GDPR. *„Pokud se dozorový úřad domnívá, že by zamýšlené zpracování uvedené v odstavci 1 porušilo toto nařízení, zejména pokud správce nedostatečně určil či zmírnil riziko, upozorní na to správce a případně zpracovatele údajů písemně ve lhůtě nejvýše osmi týdnů od obdržení žádosti o konzultaci a může uplatnit kteroukoli ze svých pravomocí uvedených v článku 58.“*[56] Stanovenou lhůtu může dozorový úřad v případě složitosti věci prodloužit o šest týdnů, o čemž musí správce informovat, stejně jako o důvodech prodloužení lhůty. **Lze vyjádřit pochybnost nad smysluplností institutu předchozí konzultace**, k níž má dojít pouze v případech, kdy správce dospěje k závěru, že zamýšlené zpracování osobních údajů představuje vysoké riziko pro základní práva a svobody fyzických osob a že toto riziko nelze zmírnit přiměřenými prostředky zajišťujícími náležitou úroveň bezpečnosti a důvěrnosti a zohledňujícími stav techniky a náklady na provedení.[57] **Lze důvodně předpokládat, že dozorové úřady budou v těchto případech spíše přistupovat k zakazování požadovaných zpracování osobních údajů** než k využití jiných možností uvedených v čl. 58 GDPR.[58]

Pověřenec pro ochranu osobních údajů

Obecné nařízení nově upravuje institut pověřence pro ochranu osobních údajů, který má být **osobou s odbornými znalostmi v oblasti právních předpisů týkajících se ochrany osobních údajů a který bude nápomocen správci a zpracovateli při zajištění souladu zpracování osobních údajů s obecným nařízením**.[59] Správce a zpracovatel je povinen jmenovat pověřence pro ochranu osobních údajů v případech, kdy zpracování provádí orgán veřejné moci či veřejnoprávní subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí; kdy hlavní činnost správce nebo zpracovatele spočívá ve zpracovávání údajů, které kvůli své povaze, rozsahu nebo účelu vyžaduje pravidelné a systematické monitorování subjektů údajů; nebo kdy hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9 GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů ve smyslu čl. 10 GDPR.[60] Členským státům je navíc dána možnost, aby nad rámec GDPR stanovily případy, kdy jsou správci nebo zpracovatelé povinni jmenovat pověřence pro ochranu osobních údajů.[61] Stejně tak je možné, aby správce nebo zpracovatel přistoupil ke jmenování pověřence pro ochranu osobních údajů zcela dobrovolně, na základě svého vlastního uvážení.

Pověřenec pro ochranu osobních údajů může být buď zaměstnancem správce, nebo může plnit své úkoly na základě smlouvy o poskytování služeb.[62] V každém případě by však pověřenci pro ochranu osobních údajů *„měli být schopni plnit své povinnosti a úkoly nezávislým způsobem“*.[63] Účelem institutu pověřence pro ochranu osobních údajů je zajistit nezávislé a do jisté míry autonomní plnění úkolů svěřených mu v ust. čl. 39 GDPR, přičemž správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny ohledně plnění svých úkolů.[64] Dále, pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím zaměstnancům správce nebo zpracovatele.[65]

Z pohledu základních pracovněprávních vztahů je třeba podotknout, že charakteristika pověřence pro ochranu osobních údajů, který bude zaměstnancem správce nebo zpracovatele, jako nezávislého a nepodléhajícího pokynům správce (nebo zpracovatele) coby zaměstnavatele, je z pohledu teorie pracovního práva přinejmenším problematická. Stejně tak je nejasný vzá-

53 Viz čl. 35 odst. 1 GDPR.

54 Viz čl. 35 odst. 2 GDPR.

55 Viz Article 29 – Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is *„likely to result in a high risk“* for the purposes of Regulation 2016/679. WP 248 [online], Brussel: European Commission, 2017, 21 str. [cit. 10. 7. 2017]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=25834.

56 Viz čl. 36 odst. 2 věta první GDPR.

57 Viz bod odůvodnění (83) a (84) GDPR.

58 Podobně také M. Nulíček a kol., op. cit. sub 3, str. 326.

59 Viz bod odůvodnění (97) GDPR.

60 Viz čl. 37 odst. 1 GDPR. Je na správci, aby na základě provedené analýzy posoudil, zda v jeho případě existuje obecným nařízením nebo právem členského státu předvídaný důvod pro jmenování pověřence pro ochranu osobních údajů. Předmětná analýza by měla být součástí dokumentace vyhotovované správcem v souvislosti s naplňováním zásady odpovědnosti ve smyslu čl. 24 GDPR. Viz Pracovní skupina podle čl. 29, Vodítka k pověřencům pro ochranu osobních údajů, WP 243 rev.01 [online], Brusel: Evropská komise, 2016, rev. 2017 [cit. 11. 7. 2017]. Dostupné z: https://www.uoou.cz/VismoOnline _ActionScripts/File.ashx?id_org=200144&id_dokumenty=23463.

61 Viz čl. 37 odst. 4 GDPR.

62 Viz čl. 37 odst. 6 GDPR.

63 Viz bod odůvodnění (97) GDPR.

64 Viz čl. 38 odst. 3 GDPR. Srov. rovněž čl. 38 odst. 6 GDPR týkající se konfliktu zájmů.

65 Viz čl. 38 odst. 3 GDPR.

jemný vztah mezi požadavkem na nezávislost a nepodřízenost pověřence pro ochranu osobních údajů pokynům správce nebo zpracovatele na straně jedné a vlastní odpovědností správce za zpracování osobních údajů v souladu s GDPR na straně druhé, neboť ani v důsledku jmenování pověřence pro ochranu osobních údajů se správce nezbavuje své odpovědnosti ve smyslu čl. 5 GDPR.[66]

Rovněž není jasné, jakým způsobem má být interpretováno ustanovení, které zakazuje rozvázání a sankcionování pracovního poměru pověřence pro ochranu osobních údajů *„v souvislosti s plněním svých úkolů“*,[67] a zda bude výpověď daná pověřenci pro ochranu osobních údajů v rozporu s tímto ustanovením GDPR, ovšem jinak vyhovující příslušným ustanovením zák. práce, v případě podané žaloby zaměstnance uznána jako neplatná dle ust. § 69 a násl. zák. práce. Vzhledem k tomu, že zák. práce je ve vztahu ke GDPR speciálním právním předpisem, je třeba splnění podmínek pro platné skončení pracovního poměru posuzovat dle jeho příslušných ustanovení. Dále, pokud GDPR v citovaném ust. čl. 38 odst. 3 hovoří o *„plnění“* úkolů, nemělo by být vyloučeno ukončení pracovního poměru pověřence pro ochranu osobních údajů v takových situacích, samozřejmě za dodržení podmínek stanovených zák. práce, kdy pověřenec pro ochranu osobních údajů neplní své úkoly řádně, včas, nebo postupuje v rozporu s GDPR, anebo pokud svým jednáním způsobí správci nebo zpracovateli jakožto svému zaměstnavateli škodu.

Z výše uvedeného důvodu lze polemizovat se striktním konstatováním, že pověřenec pro ochranu osobních údajů *„… nemůže být propuštěn a sankcionován za výkon své funkce…“*,[68] neboť za splnění podmínek stanovených zák. práce pro výpověď danou zaměstnavatelem[69] by měl být tento způsob skončení pracovního poměru jednoznačně připuštěn, navíc za situace, pokud nebude možné s ohledem na konkrétní okolnosti případu (kupř. vzhledem k výši způsobené škody) na zaměstnavateli jakožto správci nebo zpracovateli spravedlivě požadovat, aby zaměstnance na funkci pověřence pro ochranu osobních údajů dále zaměstnával. Ještě více diskutabilní by se jevil závěr, že by nebylo možné ve smlouvě o poskytování služeb, na základě níž by pověřenec pro ochranu osobních údajů svoji funkci vykonával, sjednat možnost výpovědi smlouvy správcem nebo zpracovatelem v případě porušení povinností pověřence pro ochranu osobních údajů a jeho konání v rozporu s obecným nařízením. Byť lze pochopit záměr GDPR vedoucí ke stabilní a nezávislé funkci pověřence pro ochranu osobních údajů,[70] nelze připustit výklad ustanovení GDPR takovým způsobem, že tato budou v příkrém rozporu s oprávněnými zájmy správců a zpracovatelů. Ostatně, nikoliv řádně pracující pověřenec pro ochranu osobních údajů již zcela jistě není onou zamýšlenou pojistkou ochrany osobních údajů, ale může mít naprosto opačný účinek.

Právní prostředky ochrany dle GDPR

Obecné nařízení přichází s detailní úpravou právních prostředků ochrany jak subjektů údajů, tak správců, zpracovatelů a dalších fyzických či právnických osob. Není třeba pochybovat o tom, že tyto právní prostředky ochrany budou moci využít rovněž subjekty základních pracovněprávních vztahů.

Na základě ust. čl. 77 má subjekt údajů právo, aniž by byly dotčeny jakékoliv jiné prostředky správní nebo soudní ochrany,[71] **podat stížnost u dozorového úřadu** v případě, pokud se domnívá, že zpracování jeho osobních údajů je v rozporu s GDPR.[72] K prošetření podané stížnosti je místně příslušný kterýkoliv z dozorových úřadů členských států, ale pravidlem bude dozorový úřad zvolený subjektem údajů dle jeho obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k tvrzenému porušení GDPR. Dozorový úřad je povinen subjekt údajů informovat o pokroku v řešení jeho stížnosti, jeho výsledku,[73] jakož i o možnosti soudní ochrany dle čl. 78 GDPR.

V této souvislosti je třeba upozornit na ust. čl. 78 odst. 2 GDPR, které stanoví, že v případě, kdy dozorový úřad subjekt údajů neinformuje o pokroku v řízení či jeho výsledku do tří měsíců ode dne podání stížnosti, má subjekt údajů právo na účinnou soudní ochranu. Uvedené ustanovení se jeví být do určité míry zavádějící, neboť svádí k výkladu, že se subjekty údajů mohou domáhat soudní ochrany teprve po marném uplynutí uvedené tříměsíční lhůty. Takový výklad by však byl nesprávný, neboť samotné ust. čl. 77 GDPR ve svém prvním odstavci stanoví, že institut stížnosti se nikterak nedotýká jakýchkoliv jiných prostředků správní nebo soudní ochrany. Z uvedeného důvodu je třeba ust. čl. 78 odst. 2 GDPR interpretovat tak, že **subjekt údajů se může po marném uplynutí tříměsíční lhůty bránit soudní cestou proti nečinnosti dozorového úřadu**.[74]

Právo na účinnou soudní ochranu, aniž by bylo dotčeno právo na správní či mimosoudní ochranu, proti právně závaznému rozhodnutí dozorového úřadu je dle čl. 78 GDPR přiznáno nejen subjektům údajů,[75] ale každé fyzické a právnické osobě,

66 K tomu viz Pracovní skupina podle článku 29, Vodítka k pověřencům pro ochranu osobních údajů. WP 243 rev.01 [online], Brusel: Evropská komise, 2016, rev. 2017 [cit. 11. 7. 2017]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23463.

67 Viz čl. 38 odst. 3 věta druhá GDPR.

68 Viz M. Nulíček a kol., op. cit. sub 3, str. 345.

69 Viz § 52 zák. práce.

70 Viz Pracovní skupina podle článku 29, Vodítka k pověřencům pro ochranu osobních údajů. WP 243 rev.01 [online], Brusel: Evropská komise, 2016, rev. 2017 [cit. 11. 7. 2017]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23463.

71 V této souvislosti je vhodné upozornit na právo zaměstnance podat stížnost na výkon práv a povinností vyplývajících z pracovněprávních vztahů, kterou je na základě ust. § 276 odst. 9 zák. práce zaměstnavatel povinen projednat se zaměstnancem nebo na jeho žádost s odborovou organizací.

72 K tomu srov. § 29 odst. 1 písm. c) ZOOÚ, dle něhož ÚOOÚ *„přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení“*.

73 Způsob vyřízení stížnosti se odvíjí od pravomocí dozorového úřadu vymezených v čl. 58 GDPR, přičemž jednou z možností je podle okolností jednotlivého případu uložení správní pokuty dle čl. 58 odst. 2 písm. i) ve spojení s čl. 83 GDPR.

74 V českém právním prostředí půjde o žalobu na ochranu proti nečinnosti správního orgánu ve smyslu ust. § 79 zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů (dále jen „s. ř. s.“). K tomu více viz M. Nulíček a kol., op. cit. sub 3, str. 471 a násl.

75 Toliko subjekty údajů jsou však oprávněny se soudní cestou bránit proti nečinnosti dozorového úřadu dle čl. 78 odst. 2 GDPR, o čemž bylo pojednáno výše.

které se toto rozhodnutí týká. Pro rozhodování těchto sporů je místně příslušný soud dle sídla dozorového úřadu, o jehož rozhodnutí se v dané věci jedná.[76]

Ust. čl. 79 GDPR upravuje právo na účinnou soudní ochranu vůči správci nebo zpracovateli, které je přiznáno subjektu údajů, pokud má za to, že jeho práva vyplývající z GDPR byla porušena v důsledku zpracování jeho osobních údajů v rozporu s GDPR. K rozhodování tohoto sporu je místně příslušný soud dle místa sídla provozovny správce nebo zpracovatele nebo dle místa obvyklého bydliště subjektu údajů, nejedná-li se o správce nebo zpracovatele, který je orgánem veřejné moci jednajícím v rámci výkonu veřejné moci. Prostřednictvím podané civilněprávní žaloby[77] se subjekt údajů může domáhat jak nároků odvíjejících se z ustanovení obecného nařízení, zejména pak z čl. 15 až 22 GDPR (viz výše), tak náhrady újmy dle ust. čl. 82 GDPR.[78]

Dle ust. čl. 82 odst. 1 GDPR platí, že kdokoliv utrpěl v důsledku porušení GDPR hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele plnou a účinnou náhradu utrpěné újmy.[79] Zatímco správce je odpovědný za újmu způsobenou zpracováním porušujícím GDPR, zpracovatel je odpovědný za újmu způsobenou zpracováním toliko v případě, pokud nesplnil povinnosti uložené přímo zpracovateli[80] nebo jestliže jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.[81] Jak odpovědnost správce, tak odpovědnost zpracovatele je odpovědnostní objektivní, tedy nikoliv závislou na zavinění správce či zpracovatele. Ve smyslu ust. čl. 82 odst. 3 GDPR se může jak správce, tak zpracovatel své odpovědnosti zprostit pouze v případě, *„pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla“*.[82] Lze předpokládat, že důvody pro zproštění odpovědnosti budou soudy posuzovány velmi přísně a spíše restriktivně.[83] Správce a zpracovatel odpovídají za způsobenou škodu společně a nerozdílně, přičemž následně se mohou v rámci regresního nároku vzájemně vypořádat dle podílu na odpovědnosti za vznik újmy.[84]

Závěr

Předmětem tohoto článku bylo – vzhledem k jeho omezenému rozsahu – nastínit pouze některé změny, které obecné nařízení přináší a které se promítnou mj. v pracovněprávních vztazích. S ohledem na nové společenské a technologické podmínky lze změnu právního základu ochrany osobních údajů přivítat, ovšem je otázkou, nakolik předmětné GDPR skutečně nastoluje jasná a srozumitelná pravidla chování zúčastněných subjektů a zda bude dosaženo vytyčeného cíle zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv v souvislosti se zpracováním osobních údajů.

Na základě detailního studia GDPR lze spíše nabýt dojmu, že mnohá ustanovení jsou nejednoznačná a plná vágních a blíže nespecifikovaných pojmů, přičemž jejich interpretace a bližší vymezení bude nelehkým úkolem Evropského sboru pro ochranu osobních údajů, jednotlivých dozorových úřadů a v neposlední řadě soudů členských států v následujících měsících či spíše letech.

Pokud se jedná o pracovněprávní vztahy, zde nelze odhlédnout od skutečnosti, že v této oblasti budou i nadále mezi členskými státy existovat rozdíly, předvídané a umožněné samotným GDPR, a tak nelze očekávat, že by v oblasti zpracování osobních údajů v základních pracovněprávních vztazích mělo dojít ke sjednocení přístupů všech členských států. ✤

76 Viz čl. 78 odst. 3 GDPR. V rámci české právního řádu bude procesním prostředkem k uplatnění práv žaloba proti rozhodnutí správního orgánu podaná dle ust. § 65 a násl. s. ř. s.

77 Viz § 79 a násl. zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů (dále jen „o. s. ř.“).

78 Tím však není vyloučena např. žaloba z titulu ochrany osobnosti dle o. z.

79 Viz čl. 82 odst. 1 GDPR a bod odůvodnění (142) GDPR.

80 Viz čl. 28 GDPR.

81 Viz čl. 82 odst. 2 GDPR.

82 Viz čl. 82 odst. 3 GDPR.

83 K tomu viz M. Nulíček a kol., op. cit. sub 3, str. 480-481.

84 Viz čl. 82 odst. 4 a 5 GDPR.

GDPR v otázkách a odpovědích

Za uplynulý rok se zvedl mezi odbornou veřejností a zástupci soukromého i veřejného sektoru velký zájem o nové nařízení č. 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR"). Některé dotazy, se kterými se na redakci i své poradce čtenáři obracejí, se velmi často opakují. Proto jsme se rozhodli, že sepíšeme ty nejčastější z nich a poskytneme k nim krátké a praktické odpovědi.

Mgr. Michal Nulíček, LL.M., Mgr. Kristýna Kovaříková, Mgr. et Mgr. Ing. Jan Tomíšek, Oliver Švolík

působí společně v AK Rowan Legal v Praze.

Bude třeba získat souhlas pro veškerá zpracování osobních údajů?

Již dle současné právní úpravy platí, že **souhlas není nezbytný pro každé zpracování osobních údajů. Kromě souhlasu je totiž možné zpracovávat osobní údaje na základě jiných právních základů.** Těmito právními základy jsou např. dodržení právní povinnosti správce nebo nezbytnost pro plnění smlouvy. V důsledku nepřesné implementace směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice 95/46") bohužel v českém zákoně č. 101/2001 Sb., o ochraně osobních údajů (dále jen „ZOOÚ"), vznikla formulace, která vyvolává nesprávný dojem, že souhlas je primárním právním základem a ostatní právní základy by měly být využity pouze v případě, že souhlas nelze získat. Díky tomu je dnes souhlas v mnoha případech v českém prostředí vyžadován nadbytečně, což může v některých případech vyvolávat dokonce protiprávní situaci.[1]

S GDPR se tento systém právních základů nemění. **V rámci tohoto systému by však měl každý správce nejprve pečlivě posoudit, zda může zpracovávat osobní údaje na základě jiného právního základu, a na souhlas spoléhat pouze v případě, že to možné není.** Uvažování by tedy mělo být přesně opačné, než jaké je v mnoha případech dnes, přičemž velké množství zpracování (typicky zpracování týkající se samotné podstaty podnikání správce) bude možné činit na základě nezbytnosti pro uzavření či plnění smlouvy. Další zpracování, které je nutné provádět např. v roli zaměstnavatele, bude možné provádět částečně na stejném základě, částečně na základě nezbytnosti pro plnění právních povinností. Velká množina zpracování bude v neposlední řadě prováděna na základě oprávněného zájmu – do této skupiny lze zařadit např. provozování kamerových systémů nebo některé druhy přímého marketingu.

Souhlas by měl být i nadále vyžadován v případech, kdy se jedná o zpracování, které je pro fyzické osoby, jejichž osobní údaje jsou zpracovány (dále jen „subjekty údajů"), určitým způsobem rizikové a nelze pro něj využít jiný právní titul. Z tohoto důvodu bude nutné souhlas získávat např. pro předávání osobních údajů jiným správcům pro marketingové účely nebo pro pokročilé marketingové analýzy.

Jak má podle GDPR souhlas vypadat? Musí být výslovný? Budou stávající souhlasy po účinnosti GDPR neplatné?

GDPR zvyšuje nároky na získávání souhlasu. To však neznamená, že by souhlas se zpracováním běžných osobních údajů musel být výslovný. Z definice souhlasu dle GDPR vyplývá, že **souhlas musí být svobodný, konkrétní, informovaný a jednoznačný, přičemž udělen musí být prohlášením či jiným zjevným potvrzením. Pokud souhlas nebude mít jednu z těchto kvalit, bude neplatný.**

Aby byl souhlas konkrétní, musí být udělen vždy pro konkrétní účel, který je dostatečně specifický na to, aby z něj subjekt údajů získal nějakou představu o tom, jak bude s jeho osobními údaji nakládáno. V případě, že bude účel vymezen příliš vágně, je pravděpodobné, že souhlas nebude dostatečně konkrétní.

Případů, kdy je možné považovat souhlas za nesvobodný, je více. V první řadě zde hraje roli tzv. zákaz *take-it-or-leave-it* zakotvený v čl. 7 odst. 4 GDPR, který stanoví, že poskytnutí služby nelze podmiňovat udělením souhlasu se zpracováním, které není pro takovou službu nezbytné. V praxi to znamená, že pokud chce např. internetový obchodník získávat souhlas s nabízením zboží a služeb, nesmí podmiňovat svoje plnění tímto souhlasem a musí dát svým zákazníkům skutečnou možnost jej neudělit. Mimo jiné i z tohoto důvodu jsou *a priori* neplatné všechny souhlasy, které jsou součástí obchodních podmínek, u kterých subjekt údajů nemá možnost volby. Dalšími případy, kdy je předpoklad svobodně uděleného souhlasu menší, je souhlas udělený subjektem ve slabším postavení – typicky zaměstnancem zaměstnavateli nebo občanem veřejnému orgánu.[2] **Obecným klíčem pro rozpoznání toho, kdy je a kdy není udělený souhlas svobodný, je skutečnost,**

1 Viz Stanovisko ÚOOÚ ze srpna 2014 č. 3/2014 k nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22531.

2 Bod 43 odůvodnění GDPR.

zda hrozí subjektu údajů za neudělení souhlasu nějaká újma.[3] Pokud taková újma nehrozí, je pravděpodobné, že souhlas svobodně udělen byl.

Informovaný je souhlas tehdy, pokud subjekt údajů obdržel před jeho udělením veškeré informace podle čl. 13 GDPR. Tyto údaje musí být navíc v souladu s čl. 12 GDPR sděleny transparentně, srozumitelně a za použití jasných a jednoduchých jazykových prostředků. Rovněž samotná písemná žádost o poskytnutí souhlasu má stanoveny formální náležitosti, kdy podle čl. 7 odst. 2 GDPR musí být taková žádost jasně odlišitelná od jiných skutečností, musí být srozumitelná a snadno přístupná opět za použití jasných a jednoduchých jazykových prostředků. Odchylka od těchto formálních náležitostí bude mít za následek nezávaznost té části prohlášení o souhlasu, která trpí vadami.

V neposlední řadě **musí být souhlas udělen zjevným potvrzením**. **To však neznamená, že by musel být výslovný.** Postačí, pokud subjekt údajů učiní nějakou akci, ze které je zjevné, že má v úmyslu souhlas udělit. Může se jednat o zaškrtnutí políčka (které by však nemělo být zaškrtnuto předem) či podpis, ale např. také o vyplnění e-mailové adresy do pole, u kterého je uvedeno, že si subjekt údajů přeje zasílat reklamní sdělení. **Uvedené se však neuplatní pro citlivé osobní údaje, kde v souladu se stávající právní úpravou zůstal zachován požadavek výslovnosti.**

Co se týče **platnosti souhlasů, které byly a ještě budou uděleny před účinností GDPR, ty budou platné i nadále pouze v případě, že způsob jejich udělení splňuje veškeré výše uvedené předpoklady** (s výjimkou splnění informační povinnosti v rozsahu čl. 13 GDPR). **V rámci naší praxe se však v naprosté většině případů setkáváme s tím, že souhlasy platné nejsou. Častým důvodem neplatnosti je přitom zakotvení souhlasu v obchodních podmínkách či nepřehledné zahrnutí souhlasu mezi jiná nesouvisející prohlášení.**

Ohledně požadavků na souhlas by měla Pracovní skupina podle článku 29 (WP29) na podzim vydat své výkladové stanovisko. Do té doby lze pro posouzení platnosti doposud udělených souhlasů doporučit zejména checklist, který je obsažen v pokynech k souhlasu od britského dozorového úřadu, ICO.[4]

? Co lze dělat s osobními údaji, když dojde k odvolání souhlasu? Vyžaduje GDPR vždy vymazat všechny údaje, k jejichž zpracování již správce nemá souhlas? Co dělat v případě záloh, u kterých není výmaz technicky proveditelný bez toho, aby došlo ke ztrátě jiných osobních údajů?

Pokud dojde k odvolání souhlasu, neznamená to vždy nutnost dané osobní údaje vymazat. Takové osobní údaje totiž mohou být zpracovávány zároveň pro více účelů, resp. na základě více titulů. Např. jméno a příjmení zákazníka můžeme zpracovávat v jednu chvíli pro účely splnění závazku z kupní smlouvy, pro účely nabízení zboží a služeb, pro účely archivnictví a pro účely vymáhání případných nároků. Pokud by zákazník odvolal souhlas se zpracováním osobních údajů pro účely nabízení zboží a služeb, **je možné uchovávat jméno a příjmení i nadále, dokud nepominou i všechny další účely zpracování**. Tyto další účely jsou totiž založeny na jiném právním základě, a proto odvolání souhlasu nevyvolá nezbytnost vymazání údajů.

V případě, že již nezbude skutečně žádný účel zpracování v bezsouhlasovém režimu, je nutné osobní údaje zlikvidovat. Ani to však nemusí znamenat nutnost údaje zcela smazat. Z dikce ust. čl. 5 odst. 1 písm. e) GDPR vyplývá, že je zakázáno uchovávat osobní údaje ve formě umožňující identifikaci. **Pokud tedy dojde k úspěšné anonymizaci osobních údajů, je možné nakládat s takovými údaji i nadále a GDPR se na ně vůbec nepoužije.** Takové údaje již sice není možné přiřadit ke konkrétním zákazníkům, nicméně mohou být využity pro nejrůznější analýzy trendů apod.

Specifická je také otázka osobních údajů, které společnost již k ničemu nevyužívá, ale z nějakého důvodu je nemůže vymazat. Takovým případem může být např. situace, kdy jsou na nepřepisovatelném médiu (např. na magnetické pásce) uloženy osobní údaje, které by měly být vymazány, spolu s jinými údaji, které vymazány být nemají. Výmaz jedněch osobních údajů přitom není technicky možný bez toho, aby byly vymazány i ostatní údaje. V tomto směru se kloníme k názoru britského ICO, dle kterého je možné tyto údaje (které správce sice drží, ale již je nevyužívá) nadále ponechat pasivně uložené, avšak správce nesmí údaje využít, ani mít takový úmysl, nesmí umožnit třetím stranám přístup k takovým osobním údajům, musí zajistit vhodná organizační a technická bezpečnostní opatření a musí být rozhodnut a připraven, jakmile to bude technicky možné, osobní údaje vymazat.[5]

? Bude možné zpracovávat osobní údaje z veřejných rejstříků či sociálních sítí?

Využití údajů zveřejněných ve veřejných rejstřících, či dokonce údajů, které o sobě mnozí zveřejňují na sociálních sítích, je pro mnohé správce velmi lákavé. Jako příklady takových užití lze uvést zasílání marketingových nabídek osobám, které jsou uvedeny v obchodním rejstříku jako jednatelé společností, nebo užití údajů ze sociálních sítí v rámci hodnocení uchazečů o zaměstnání.

V každém případě dalšího využití zveřejněných osobních údajů je však nutné zohlednit účel, za kterým byly takové osobní údaje původně zveřejněny. Není možné je užívat bez dalšího pro jakýkoliv účel a jakýmkoliv způsobem – takové další užití musí splnit test slučitelnosti účelů dle čl. 6 odst. 4 GDPR. V rámci tohoto testu jsou posuzovány např. vzájemný vztah původního a nového účelu zpracování, možná rizika pro subjekty údajů spojená s novým zpracováním či bezpečnostní záruky (např. pseudonymizace) přijaté za účelem zabránění zásahu do práv a oprávněných zájmů subjektů údajů v rámci nového zpracování.

Pokud bude výsledek testu slučitelnosti účelů pozitivní, neznamená to automaticky, že je cesta ke zpracování zcela otevřená. **Vedle účelu je totiž nutné zajistit pro další zpracování zveřejněných údajů i právní základ.** V převážné většině přípa-

3 Bod 42 odůvodnění GDPR.

4 Viz Information Commissioner's Office, Consultation: GDPR consent guidance. Dostupné z: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

5 Viz Information Commissioner's Office, Deleting personal data. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf, str. 5.

dů, kdy je zamýšleno zpracovávat osobní údaje z veřejných zdrojů, bude tímto právním základem **oprávněný zájem správce**.

Stejně jako zkoumání slučitelnosti účelů, vyžaduje i samotný oprávněný zájem provedení posouzení, v tomto případě toho, zda základní práva a zájmy subjektů údajů nepřeváží nad oprávněným zájmem správce. V rámci tohoto posouzení (balančního testu) je nutné vzít do úvahy více faktorů, a to především váhu samotného oprávněného zájmu, možné negativní či pozitivní důsledky pro subjekty údajů, rozumné očekávání subjektů údajů ohledně zpracování či vztah správce a subjektu údajů. I výsledek balančního testu lze nakonec ovlivnit ve prospěch správce také přijetím vysokých záruk bezpečnosti zpracování či vyšší transparentností zpracování. Posouzení oprávněného zájmu je zároveň nutné pečlivě dokumentovat a být připraven jej v souladu se zásadou odpovědnosti předložit Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ") ke kontrole.

Jak vyplývá z výše uvedeného, **pro zpracování údajů z veřejných zdrojů je třeba vždy provést posouzení slučitelnosti účelů a (pokud je další zpracování založeno na oprávněném zájmu) balanční test oprávněného zájmu**. S ohledem na slučitelnost účelů a rozumné očekávání subjektů údajů je přitom např. pravděpodobné, že osobní údaje z obchodního rejstříku mohou být využity pro kontrolu pravdivosti identifikačních údajů v rámci obchodního styku, o něco méně pravděpodobná je oprávněnost využití kontaktních údajů osob, které jsou v rejstřících uvedeny, pro účely marketingu. Jak je však z výše uvedených kritérií patrné, konečný závěr vždy vyžaduje důkladnou analýzu.

? Jaké jsou dopady GDPR do oblasti marketingu?

Pro řadu organizací je marketing a prodej oblastí, ve které má GDPR největší dopad. Význam těchto dopadů závisí na druhu marketingových aktivit, které daná organizace realizuje, ale také na tom, v jaké míře jsou tyto aktivity prováděny v souladu již se současnou právní úpravou.

GDPR v bodu 47 svého odůvodnění stanoví, že *„zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu"*. To znamená, že do určité míry je možné osobní údaje pro účely přímého marketingu zpracovávat i bez souhlasu subjektů údajů. Tato možnost však není bezbřehá, tato výjimka bude podle našeho názoru naopak vykládána spíše restriktivně. Oprávněný zájem správce je tedy třeba v každém případě samostatně posoudit a bude dán zejména tam, kde existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem, např. pokud je subjekt údajů zákazníkem správce. Klíčové pro posouzení oprávněného zájmu je zejména to, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít. [6]

V praxi je tedy na základě oprávněného zájmu a bez souhlasu subjektu údajů možné provádět zejména zpracování osobních údajů za účelem přímého marketingu vlastních produktů a služeb stávajícím zákazníkům,[7] např. formou cílené reklamy v klientské zóně na webových stránkách či formou klasického dopisu. Souhlasem pak budou typicky podmíněny pokročilé marketingové aktivity jako sledování a vyhodnocování aktivity jednotlivých zákazníků na webových stránkách a obohacování údajů o zákaznících z dalších zdrojů (např. ze sociálních sítí) za účelem lepšího cílení reklamy.[8]

V kontextu šíření marketingu elektronickými prostředky (telefonní marketing, rozesílání e-mailů a textových zpráv s reklamním obsahem) je však výše uvedené třeba vnímat jako podmínky pro personifikaci *obsahu* reklamního sdělení, přičemž další podmínky se budou vztahovat na *využití příslušného elektronického kanálu*.

Tyto další podmínky stanoví zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů (dále jen „ZSIS"), který má být nahrazen nařízením e-Privacy (zatím ve fázi návrhu) [9]

Podle § 7 ZSIS, stejně jako dle čl. 13 e-Privacy, je možné šířit obchodní sdělení pouze se souhlasem příjemce. Výjimkou je zasílání nabídek obdobných produktů a služeb elektronickou poštou na kontakty, které správce získal v souvislosti s prodejem svého zboží a služeb. V takovém případě je možné zasílání nabídek bez souhlasu v tzv. režimu opt-out, tedy za podmínky, že správce při získání kontaktu a při každém dalším obchodním sdělení umožní adresátovi jednoduchým způsobem zdarma zasílání nabídek odmítnout.[10] Tato výjimka pokrývá obchodní sdělení zaslaná formou e-mailu či textové zprávy,[11] nevztahuje se však na telefonní marketing, který podléhá souhlasu vždy.[12]

Na tomto místě je vhodné podotknout, že připravované nařízení e-Privacy mění také režim pro umísťování cookies na zařízení uživatele.[13] Pro umístění cookies, které nejsou nezbytné pro fungování dané webové stránky (např. pro přihlášení apod.) nebo pro měření návštěvnosti, bude nezbytný předchozí souhlas uživatele, přičemž na takový souhlas jsou kladeny obdobné požadavky, jako obsahuje GDPR. Doplňujeme, že dle platné právní úpravy (nepřesně implementující příslušnou evropskou směrnici) je v České republice (zatím) dostatečné, pokud má uživatel možnost umístění cookie odmítnout.[14]

6 K posouzení oprávněného zájmu blíže viz M. Nulíček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek: GDPR/Obecné nařízení o ochraně osobních údajů, Praktický komentář, Wolters Kluwer, Praha 2017, str. 132. Viz též Pracovní skupina pro ochranu údajů zřízená podle článku 29: Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES, 9. 4. 2014, dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf, str. 30.

7 Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29, op. cit. sub 6, str. 25.

8 Viz též Pracovní skupina pro ochranu údajů zřízená podle článku 29, op. cit. sub 6, str. 26.

9 Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final – 2017/03 (COD). Dostupné z: http://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX:52017PC0010.

10 Viz § 7 odst. 3 ZSIS.

11 Viz M. Maisner: Zákon o některých službách informační společnosti: komentář, C. H. Beck, Praha 2016, str. 2.

12 Přehledný výklad k problematice přímého marketingu pomocí elektronických komunikací poskytuje např. stanovisko britského ICO k této problematice, viz Information Commissioner's Office: Direct marketing, dostupné z: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf.

13 K fungování cookies blíže viz např. J. Donát, J. Tomíšek: Právo v síti: průvodce právem na internetu, C. H. Beck, Praha 2016, str. 11.

14 Viz § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. Tato úprava je však již nyní v rozporu s požadavky směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

Ačkoliv tedy GDPR umožňuje provádět některé marketingové aktivity na základě oprávněného zájmu, bude řada marketingových aktivit podléhat souhlasu dotčené osoby, ať již z hlediska zpracování osobních údajů pro personifikaci reklamního sdělení, využití elektronického komunikačního kanálu, či z hlediska nutnosti umístit na zařízení uživatele tzv. sledovací cookie. S ohledem na přísnější požadavky, které GDPR na souhlas klade, přitom řada dosud získaných marketingových souhlasů po účinnosti GDPR neobstojí.

Z toho pro správce zpravidla plyne nutnost upravit stávající formu získávání marketingových souhlasů (jak v listinné formě např. při uzavírání smlouvy v bance, tak elektronicky např. při nákupu na e-shopu) a současně praktická nutnost získat nové marketingové souhlasy od osob, jejichž údaje správce již v minulosti pro tento účel získal. Protože však nelze očekávat, že správce bude při získávání nových souhlasů od stávajících subjektů údajů 100% úspěšný, je třeba se připravit i na scénář, kdy souhlas nebude udělen. Ve vztahu k takovým osobám je třeba ukončit a v budoucnu neprovádět zpracování, které je souhlasem podmíněno, včetně likvidace údajů, pro jejichž zpracování nemá správce jiný právní základ. Stejně tak je třeba ukončit zasílání obchodních sdělení elektronickou poštou osobám, jejichž kontakt správce získal při prodeji svého zboží či služby, ale nemá jejich souhlas, ani jim neumožnil zasílání obchodních sdělení snadno odmítnout.

? Je dle GDPR možné k marketingovým účelům využívat databáze kontaktů poskytnuté třetí stranou?

Častou praxí zejména v e-mailovém a telefonním marketingu je využívání databází třetích stran pro získání kontaktů k oslovení v rámci marketingové komunikace. Pro tuto praxi představuje GDPR významné omezení, jak upozornil nedávno na svých webových stránkách také ÚOOÚ. Využití údajů z těchto databází třetími osobami je totiž zpravidla podmíněno souhlasem subjektu údajů. S ohledem na požadavky GDPR přitom v mnoha případech nebudou po účinnosti GDPR takové souhlasy platné, např. proto, že byly zahrnuty do všeobecných obchodních podmínek, byly podmínkou uzavření smlouvy, byly uděleny předem neurčenému počtu správců se zasíláním předem neurčeného okruhu obchodních nabídek apod.[15]

V praxi lze tedy správcům doporučit využití a zpracování pouze takových kontaktů z databází, u kterých poskytovatel databáze správci jednoznačně prokáže udělení platného souhlasu a dostatečné informování subjektu údajů o zpracování novým správcem (nabyvatelem databáze). V případě důvěryhodných partnerů může správce poskytovatele kontaktů pouze smluvně zavázat k tomu, aby souhlasy a informování doložil na vyžádání, např. v případě kontroly ze strany ÚOOÚ, a případně správce kompenzoval, když tyto souhlasy nedoloží. V takovém případě se však příslušný správce vystavuje riziku, protože z hlediska GDPR, resp. ZSIS, je za prokázání souhlasů a dostatečného informování subjektů údajů odpovědný správce, který příslušné údaje využívá pro své účely, což potvrzuje rozhodovací praxe ÚOOÚ.[16]

? Jaké bude mít GDPR dopady na oblast HR? Budou třeba nové souhlasy od zaměstnanců?

GDPR zasahuje nejenom do vztahů s klienty a do dodavatelských vztahů, ale má rovněž dopad do oblasti HR. GDPR v čl. 88 umožňuje členským státům stanovit konkrétnější pravidla v této oblasti – zatím se nezdá, že by Česká republika této možnosti chtěla využít; nicméně je vhodné připomenout, že dílčí úprava ochrany soukromí zaměstnanců je obsažena i v zákoníku práce (zejm. § 316 zák. práce).

Pokud jde o právní základ zpracování osobních údajů zaměstnanců, i nadále platí, že **nejvhodnějším právním titulem pro zpracování osobních údajů zaměstnanců je nezbytnost pro plnění pracovní smlouvy** [čl. 6. odst. 1 písm. b) GDPR] **a nezbytnost pro plnění právních povinností** [čl. 6 odst. 1 písm. c) GDPR], popř. oprávněný zájem správce [čl. 6 odst. 1 písm. f) GDPR]. Pracovněprávní předpisy přitom ukládají zaměstnavatelům celou řadu povinností (v oblasti daňové, sociálního zabezpečení a další), kdy bude právě druhý ze zmíněných titulů relevantní [čl. 6 odst. 1 písm. c) GDPR].

Naopak souhlas se zpracováním, jak také upozorňuje WP29 ve svém posledním stanovisku č. 2/2017 ke zpracování osobních údajů v zaměstnání,[17] není zpravidla vhodným právním titulem a je velice pravděpodobné, že **drtivá většina souhlasů získaných od zaměstnanců nebude platná**. Důvodem neplatnosti bude zpravidla nerovné postavení zaměstnance a zaměstnavatele, kdy je vysoká pravděpodobnost, že neudělení souhlasu bude mít pro zaměstnance negativní důsledky. Pokud by však zaměstnavatel skutečně zajistil to, že odmítnutí udělení souhlasu pro zaměstnance žádné negativní důsledky mít nebude, lze stále v omezené míře využít i tohoto právního titulu.

? Co se rozumí automatizovaným rozhodnutím dle čl. 22 GDPR?

Automatizované rozhodnutí je dle definice v čl. 22 odst. 1 GDPR rozhodnutím založeným výhradně na automatizovaném zpracování, včetně profilování, které má právní účinky na subjekt údajů nebo na něj obdobným způsobem významně dopadá. V současnosti panují odlišné názory ohledně toho, zda je nutné klást důraz na pojem „výhradně“ a vyjmout z působnosti tohoto ustanovení každé rozhodnutí, které má v sobě alespoň nominální prvek lidského zásahu, nebo jestli je nutné dbát spíše na smysl a účel tohoto ustanovení a výkladem překlenout výrazné nebezpečí zneužití.

S ohledem na to, že GDPR by mělo obecně zvýšit úroveň ochrany osobních údajů, s ohledem na výrazně ochranářský výklad poskytovaný WP29 a s ohledem na dosavadní směr výkladu podobných rozporů Soudním dvorem Evropské unie (dále jen „SDEU“) je však z důvodu opatrnosti vhodné zvolit střední cestu a přiklonit se spíše k názoru, že **čistě nominální lidský prvek v řetězci rozhodnutí k vyjmutí z působnosti tohoto ustanovení ne-**

15 ÚOOÚ: Využívat databáze k rozesílání nabídek lze jen omezeně, 30. 6. 2016, dostupné z: https://www.uoou.cz/vyuzivat%2Ddata baze%2Dk%2Dnbsp%2Drozesilani%2Dnab idek%2Dlze%2Djen%2Do mezene/d-25003. Požadavek na prokázání souhlasů vyplývá z čl. 7 odst. 2 GDPR.

16 Kontrola v oblasti šíření obchodních sdělení (Zaplo Finance s. r. o.) [online]. [cit. 2017-08-18]. Dostupné z https://www.uoou.cz/kontrola-v-oblast i-sireni-ob chodnich-sdeleni-za plo-finance-s-r-o/ds-4587/archiv=0&p1=4574.

17 Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29: Stanovisko č. 2 /2017 ke zpracování osobních údajů v zaměstnání, 8. 6. 2017, dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

stačí. Člověk, který se na rozhodnutí podílí, by měl mít alespoň částečnou kontrolu nad rozhodnutím a určitou míru autonomie.

V praxi bývá automatizované individuální rozhodování využíváno např. v pojišťovnictví při výpočtu výše pojistného či v bankovnictví při posuzování úvěrového rizika a rozhodování o přiznání či odmítnutí úvěru.

Co je dle GDPR potřeba učinit ve vztahu ke zpracovatelům, tedy subjektům, které pro správce zpracovávají osobní údaje?

Podle čl. 28 odst. 1 GDPR má správce v první řadě povinnost využívat pouze ty zpracovatele, kteří mu dají dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky GDPR a aby byla zajištěna ochrana práv subjektu údajů.

GDPR také klade nové, přísnější požadavky na smlouvy se zpracovateli osobních údajů. Ve smlouvě musí být stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie osobních údajů, a dále by měl správce zavázat zpracovatele, aby splnil požadavky dle čl. 28 odst. 3 písm. a) až h) GDPR. Zejména by měl se zpracovatelem smluvně ošetřit součinnost při výkonu práv subjektů údajů, oznamování a řešení bezpečnostních incidentů dle čl. 33 a 34 GDPR a otázku auditů, včetně inspekcí, prováděných správcem nebo auditorem, kterého správce pověří.

Každý správce by tedy měl před účinností GDPR prověřit, zda zpracovatelé, které využívá, skutečně tyto požadavky splňují a následně by to měl pravidelně prověřovat. Současně by měl revidovat smlouvy, které má s těmito zpracovateli uzavřeny, a případně je doplnit či upravit. Jelikož u velkých organizací může být počet zpracovatelů, které využívají, značný (zejména pokud pro distribuci svých produktů používají síť partnerů, kteří jsou často v postavení zpracovatele), může být revize smluv pracným a časově náročným úkolem. V praxi je proto klíčové stanovení priorit – logickým krokem je zahájit prověřování a úpravy u zpracovatelů, kteří představují pro subjekty údajů i pro správce největší riziko, např. z důvodu rozsahu zpracovávaných údajů citlivého charakteru či případně zjevně nedostatečného zabezpečení na straně zpracovatele.

Musí se dle GDPR všechny osobní údaje šifrovat?

Ačkoliv GDPR uvádí mezi bezpečnostními opatřeními v čl. 32 odst. 1 písm. a) šifrování, neznamená to, že je šifrování (či další uvedená opatření, jako např. pseudonymizace) třeba provádět u každého zpracování a pro všechny osobní údaje.

GDPR stanoví správci a zpracovateli povinnost přijmout vhodná technická a organizační opatření k zajištění integrity a důvěrnosti zpracovaných osobních údajů.[18] To, jaká opatření správce musí přijmout, záleží na posouzení rizika, které dané zpracování představuje, na stavu techniky a na nákladech na zavedení jednotlivých opatření. V tomto směru tak GDPR nepřináší žádnou změnu, stejný princip je upraven v § 13 ZOOÚ.

Novinkou je právě výčet v čl. 32 odst. 1 písm. a) až d), kde jsou uvedeny příklady bezpečnostních opatření, která by měl správce a zpracovatel v závislosti na výsledku posouzení rizika zavést.[19] GDPR nepožaduje, aby všechna tato opatření byla u každého zpracování zavedena, správce a zpracovatel by však měli jejich zavedení uvážit, a pokud se rozhodnou některé z uvedených opatření nezavést, měli by být schopni své rozhodnutí zdůvodnit.

V praxi je tedy třeba, aby každý správce a zpracovatel provedl pro své zpracování analýzu rizik, která dané zpracování představuje, a zavedl taková opatření, která vyhodnotí jako přiměřená daným rizikům, nákladům a dostupným technologiím. Přitom musí zvážit opatření vyjmenovaná v čl. 32 odst. 1 GDPR, avšak nejen je.[20] Následně je vhodné (samozřejmě vedle samotné implementace zvolených opatření) provedené posouzení přiměřeně dokumentovat, zejména za účelem splnění povinnosti prokázat (a nejen zajistit) soulad s GDPR.[21] Jelikož bezpečnostní rizika, náklady na zavedení i stav techniky se neustále mění, měli by správci a zpracovatelé do budoucna také **zavést proces pravidelného přezkumu** posuzování rizika pro bezpečnost zpracování a v případě změny okolností bezpečnostní opatření aktualizovat.

Když data neobsahují rodné číslo ani jméno a příjmení, jedná se dle GDPR o osobní údaje?

GDPR stanoví, že osobním údajem je jakákoliv informace o identifikované nebo identifikovatelné fyzické osobě.[22] V první řadě tedy není osobním údajem pouze samotný identifikátor jako rodné číslo nebo jméno a příjmení, ale veškeré informace o dané osobě, které jsou s tímto identifikátorem spojeny (např. kompletní záznam v personálním systému, který se vztahuje ke konkrétnímu zaměstnanci).

I v případě, kdy ze záznamu odstraníme všechny přímé identifikátory jako rodné číslo nebo jméno a příjmení, nemusí konkrétní záznam přestat obsahovat osobní údaje, pokud lze příslušná data přiřadit ke konkrétní fyzické osobě nepřímo. Pokud tedy např. zmíněný záznam v personálním systému obsahuje informace o věku, dosaženém vzdělání a kvalifikaci, které v rámci dané organizace odpovídají pouze jedné osobě, pak celý záznam (vč. případné výše mzdy daného zaměstnance apod.) stále představuje osobní údaje, i když jsou přímé identifikátory odstraněny.

Do jaké míry je třeba brát možnost nepřímé identifikace v potaz, stanoví bod 26 odůvodnění GDPR, dle kterého je třeba přihlédnout ke všem prostředkům, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze použití prostředků k identifikaci fyzické osoby rozumně předpokládat, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji. Správce by se přitom měl zaměřit na konkrétní prostředky, kterými lze z anonymizovaných údajů jedince zpětně identifikovat, a přihlížet k tomu, jak nákladná je tato zpětná identifikace, jestli je k ní potřeba extenzivní know-how a jaká je pravděpodobnost, že k ní dojde.

18 Viz čl. 32 odst. 1 GDPR.

19 Podobný výčet obsahuje § 13 odst. 4 ZOOÚ pro automatizované zpracování, v ZOOÚ je však zavedení uvedených stanoveno jako povinné bez ohledu na výsledek analýzy rizik.

20 K postupu analýzy rizik viz M. Nulíček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit. sub 6, str. 248 a 291.

21 Jde o tzv. zásadu odpovědnosti, viz čl. 5 odst. 2 GDPR.

22 Viz čl. 4 bod 1 GDPR.

Původní směrnice 95/46/ES[23] obsahovala obdobné ustanovení, ke kterému poskytl bližší výklad Soudní dvůr Evropské unie ve věci *Breyer*. Z rozhodnutí plyne, že možnost identifikace konkrétní osoby je třeba vnímat objektivně, a pokud existuje více než hypotetická možnost, že jiná osoba identifikaci provede, je třeba příslušná data považovat za osobní údaje. Konkrétním závěrem rozhodnutí je, že dynamická IP adresa shromažďovaná provozovatelem webové stránky je osobním údajem.[24]

V praxi tak budou osobními údaji i data, která správce upraví tak, aby neobsahovala přímé identifikátory (např. technikou tzv. hashování), a následně je předá ke zpracování třetí osobě, protože správce je schopen na základě původních dat provést zpětnou identifikaci subjektů údajů (pokud původní data neodstraní). V takovém případě se bude jednat o pseudonymizované údaje, tedy údaje chráněné bezpečnostním opatřením snižujícím riziko, které je s daným zpracováním spojeno, stále však podléhající režimu GDPR.

Pokud chce správce určitá data zcela vyjmout z režimu GDPR, je třeba provést jejich anonymizaci, v rámci které jsou data upravena takovým způsobem, že je nelze přiřadit ke konkrétní fyzické osobě, s přihlédnutím ke všem prostředkům, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby.

Anonymizace není v praxi záležitostí jediné operace. Podle stanoviska WP29 č. 5/2014 ze dne 10. 4. 2014 k technikám anonymizace[25] lze úplné anonymizace docílit jen kombinací více metod, jako je agregace, permutace či „přidání šumu". Jedině kombinací více takových opatření lze dosáhnout toho, že z datového souboru není možné vyčlenit jednotlivce, není možné propojit různé záznamy týkající se jedné osoby a z datového souboru není možné vyvodit informace týkající se jedné osoby – teprve pokud jsou tato posledně jmenovaná tři kritéria splněna, lze prohlásit, že osobní údaje jsou anonymizovány.

? Musí každá organizace pracující s osobními údaji jmenovat pověřence pro ochranu osobních údajů?

Navzdory široce rozšířenému mýtu **nemusí** dle GDPR jmenovat pověřence zdaleka každý správce nebo zpracovatel. Tuto povinnost mají pouze:

- orgány veřejné moci a veřejné subjekty, s výjimkou soudů jednajících v rámci svých pravomocí,
- správci a zpracovatelé, jejichž hlavní činnost spočívá v operacích zpracování, které kvůli své povaze, rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, a
- správci a zpracovatelé, jejichž hlavní činnost spočívá v rozsáhlém zpracování citlivých údajů nebo údajů o trestné činnosti.[26]

Pro posouzení naplnění druhých dvou podmínek je klíčový výklad pojmů hlavní činnost a rozsáhlé zpracování. WP29 pojem hlavní činnost vykládá jako takovou činnost, která je nezbytná k dosažení cílů organizace, přičemž pro naplnění podmínky postačí, když je zpracování neoddělitelnou součástí takové činnosti. Jako příklad lze uvést nemocnici, jejíž hlavní činností je poskytovat zdravotnickou péči. Takovou péči by však nemohla bezpečně a efektivně poskytovat, pokud by nezpracovávala citlivé osobní údaje svých pacientů obsažené ve zdravotnické dokumentaci, proto **bude takové zpracování osobních údajů hlavní činností nemocnice**. Na druhou stranu nebude možné považovat za hlavní činnost takové zpracování, které probíhá běžně v různých organizacích za účelem dosažení sekundárních cílů, jako je zajišťování personálních procesů či správa IT infrastruktury.[27]

Podle WP29 současně **nelze určit, které zpracování se považuje za rozsáhlé, pouze na základě jediného faktoru**. Do úvahy bude nutné brát zejména počet subjektů údajů, kterých se zpracování dotkne, objem zpracovaných údajů, dobu a stálost zpracování či geografický rozsah činností zpracování. WP29 výslovně uvádí některé **příklady rozsáhlého zpracování, mezi něž řadí např. zpracování údajů o pacientech v rámci běžného provozu nemocnice, zpracování osobních údajů o subjektech údajů v rámci systému městské hromadné dopravy nebo zpracování osobních údajů v rámci běžného provozu pojišťovny či banky**. Konkrétní hranice z hlediska počtu subjektů údajů či počtu záznamů však není stanovena.[28]

Pro naplnění poslední podmínky je pak rozhodující pojem pravidelné a systematické monitorování. Dle názoru WP29 je nutné za takové monitorování považovat jakékoliv probíhající, opakované či pravidelné, organizované či systematické sledování a profilování subjektů údajů. WP29 uvádí také konkrétní praktiky, které budou za toto monitorování považovány, mezi něž řadí např. **poskytování telekomunikačních služeb, cílení internetové reklamy pomocí e-mailu, profilování a skórování pro účely posouzení rizik apod.**[29]

V praxi lze doporučit, aby každá organizace, která alespoň potenciálně může splňovat uvedené podmínky, provedla bližší posouzení na základě konkrétních činností zpracování, které provádí. V případě, že se rozhodne pověřence (pro nesplnění kritérií pro jeho povinné jmenování) nejmenovat, měla by příslušné odůvodnění důkladně dokumentovat, aby jej mohla v případě potřeby předložit ÚOOÚ. Pokud výsledek posouzení není jednoznačný, je z hlediska prevence rizik vhodným postupem pověřence jmenovat. Je však třeba pamatovat také na to, že i pověřenec jmenovaný dobrovolně musí splňovat všechny požadavky stanovené GDPR.[30] ✤

Tématu GDPR se budeme věnovat i v následujících číslech Bulletinu advokacie.

23 Viz směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

24 Viz bod 1 výroku rozsudku SDEU ze dne 19. 10. 2016 ve věci C-582/14, *Patrick Breyer*. K pojmu IP adresa viz např. J. Donát, J. Tomíšek, op. cit. sub 13, str. 13.

25 Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29: Stanovisko č. 5 /2014 k technikám anonymizace, 10. 4. 2014, dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

26 Viz čl. 37 odst. 1 GDPR.

27 Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29: Návrh výkladového pokynu WP29 k pověřenci pro ochranu osobních údajů, 13. 12. 2016, dostupné z: http://ec.europa.eu/newsroom/document.cfm?doc_id=43823, str. 6.

28 Tamtéž, str. 7

29 Tamtéž, str. 8.

30 Pokud je prezentován v rámci organizace, na veřejnosti či vůči Úřadu jako pověřenec. To však nebrání tomu, aby organizace určila osobu či útvar odpovědný za problematiku ochrany osobních údajů, aniž by tyto osoby automaticky získaly status pověřence.

Doporučení CCBE ohledně klíčových opatření pro advokáty

k dosažení souladu s předpisy v souvislosti s GDPR

Toto doporučení, přijaté CCBE na plenárním zasedání 19. 5. 2017 v Edinburghu, je reakcí na nedávno přijatou evropskou legislativu – nařízení Evropského parlamentu a Rady č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů, tzv. GDPR) a směrnici Evropského parlamentu a Rady 2016/680 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.

Dokument se zaměřuje pouze na aspekty ochrany osobních údajů, ze kterých plynou dodatečné povinnosti. **Cílem doporučení je zajistit, aby advokátní praxe jednoduše identifikovala problémy, které je potřeba okamžitě řešit.**

Prostřednictvím tohoto dokumentu by Rada evropských advokátních komor (CCBE) chtěla uvést **přehled základních nových opatření k dosažení souladu s předpisy, která mohou advokátní komory doporučovat za účelem souladu s požadavky stanovenými GDPR**.

V následujících částech jsou zdůrazněny ty aspekty GDPR, které zejména pro advokáty nebo advokátní kanceláře (dále jen jako „advokátní praxe“) přinášejí nutnost nového nebo zvýšeného dodržování povinností plynoucích z předpisů. Účelem zdůraznění těchto záležitostí je, aby mohly advokátní praxe snadno identifikovat problémy, jimiž by se měly zabývat v první řadě. Vzhledem k tomu, že drtivá většina evropských advokátních praxí spadá pod hranici 250 zaměstnanců, níže uvedené záležitosti se netýkají ustanovení, která se vztahují pouze na větší advokátní kanceláře. Rovněž je třeba věnovat pozornost skutečnosti, že mnoho advokátních kanceláří zpracovává osobní údaje, které lze označit za „zvláštní kategorie osobních údajů“.

Ohlašování porušení zabezpečení

Podle čl. 33 je advokátní právní praxe působící jako správce údajů povinna oznámit porušení zabezpečení příslušnému dozorovému úřadu bez zbytečného odkladu, v žádném případě ne později než 72 hodin od okamžiku, kdy se o něm dozvěděla. V případě pozdějšího ohlášení je nutné uvést důvody pro zpoždění. Existuje výjimka v případě, kdy porušení zabezpečení osobních údajů pravděpodobně nezpůsobí žádnou újmu subjektu (subjektům) údajů.

Pokud advokátní praxe působí jako zpracovatel a zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

Toto oznámení musí mj. obsahovat specifikaci povahy porušení údajů (kategorie a přibližný počet dotčených subjektů údajů a záznamů osobních údajů), pravděpodobné následky porušení zabezpečení a opatření, která byla přijata nebo budou přijata ke zmírnění možných nepříznivých účinků. Oznámení lze provést v různých fázích.

Kromě toho je správce povinen tato porušení dostatečně podrobně zdokumentovat, aby dozorový úřad mohl ověřit soulad s oznámením porušení. Advokátní praxe jsou také povinny stanovit interní postupy pro řešení porušení zabezpečení údajů a zavést mechanismus pro oznamování dozorovému úřadu.

V určitých případech s vysokým rizikem je advokátní praxe rovněž povinna přímo informovat klienta (čl. 34), i když existují zvláštní výjimky.

Samotný formát oznámení, definice „zbytečného odkladu“, požadavky na obsah dokumentace a výklad limitů a výjimek dozorovými orgány se mohou mezi jednotlivými členskými státy lišit.

Advokátní praxe by tudíž měly být informovány o již existujících a možných budoucích vnitrostátních pokynech v těchto oblastech.

I když některé členské státy již do vnitrostátního práva zavedly požadavky na ohlašování porušení zabezpečení údajů, směrnice 95/46/ES neukládala, aby správci hlásili porušení zabezpečení údajů dozorovému úřadu. Tento požadavek ale již existuje v odvětví telekomunikací [viz směrnice 2002/58/ES a nařízení Komise (EU) č. 611/2013, jež se vztahují na poskytovatele služeb elektronických komunikací]. Výše uvedené prováděcí nařízení bylo definováno způsobem nezávislým na odvětví a v některých členských státech mohou dozorové úřady v oblasti telekomunikací nebo ochrany osobních údajů vydat podrobnější pokyny. Co je ještě důležitější, na základě této legislativy vydala pracovní skupina dozorových úřadů EU v oblasti ochrany osobních údajů zřízená podle čl. 29 podrobné pokyny o provádění nařízení o porušení zabezpečení údajů (stanovisko WP 213 č. 03/2014 o oznámení k narušení bezpečnosti osobních údajů, 25. 3. 2014[1]), které stanoví doporučené postupy v této oblasti pro všechny správce údajů.

Pokud jde o budoucí předpisy v této oblasti, dle čl. 70 odst. 1 písm. g) a h) GDPR vydá Evropská rada pro ochranu údajů pravděpodobně pokyny, doporučení a osvědčené postupy pro a) to, jak zjistit případy porušení zabezpečení osobních údajů, b) to, jak určit „zbytečný odklad“, a c) okolnosti, za nichž jsou správce a zpracovatel povinni porušení ohlásit dozorovému úřadu nebo klientům.

1 Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_cs.pdf.

Právo být zapomenut

Čl. 17 obsahuje právo na výmaz („právo být zapomenut"), což znamená, že subjekty údajů mají právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daných subjektů týkají. Tentýž článek ukládá správci povinnost vymazat bez zbytečného odkladu osobní údaje, nastane-li některý z důvodů uvedených v odst. 1 písm. a) až f). Toto ustanovení má původ v případu *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos, Mario Costeja González*,[2] v němž soud uvedl, že jednotlivci mají právo (za určitých podmínek a záruk) požádat, aby vyhledávače odstranily odkazy s jejich osobními údaji. Jak již ale bylo uvedeno, čl. 17 odst. 3 písm. e) obsahuje významné omezení, kterého by se mohly dovolávat advokátní praxe v souvislosti s činnostmi při zpracovávání, které jsou nezbytné „pro určení, výkon nebo obhajobu právních nároků".

Je důležité si uvědomit, že toto ustanovení samozřejmě nemá přednost před určitými vnitrostátními předpisy, které stanoví povinnost uchovávat údaje po určitou dobu (např. pro splnění daňových povinností).

Pověřenec pro ochranu osobních údajů (DPO)

Povinnost advokátních kanceláří jmenovat DPO

Další novinkou je povinnost jmenovat DPO, pokud činnosti zpracování údajů určité organizace zahrnují rozsáhlé pravidelné a systematické monitorování subjektů údajů nebo **rozsáhlé zpracování zvláštních kategorií osobních údajů** (čl. 37). Pracovní skupina zřízená podle čl. 29 (WP29), která se skládá ze zástupců orgánů pro ochranu osobních údajů členských států, vydala pokyny ohledně DPO, v nichž objasňuje jejich úlohu a uvádí doporučené postupy.

Je-li jmenován DPO, organizace musí zveřejnit jeho údaje a musí tyto údaje sdělit příslušnému dozorovému úřadu.

V čl. 9 GDPR jsou definovány zvláštní kategorie osobních údajů,[3] jejichž zpracování je zakázáno, ale s určitými výjimkami: dle čl. 9 odst. 2 písm. f) se tento zákaz nevztahuje na zpracování nezbytné „pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí". Toto ustanovení tedy povoluje zpracování zvláštních kategorií osobních údajů v kontextu práce advokátních praxí ve sporných řízeních.

Na správce a zpracovatele zvláštních kategorií údajů se ale stále vztahuje čl. 37 (a rovněž čl. 35, viz níže). Tato ustanovení vyžadují v případě, kdy hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9, *jmenování pověřence pro ochranu osobních údajů.* Podle pokynů ohledně DPO lze hlavní činnosti považovat za klíčové operace k dosažení cílů správce nebo zpracovatele. Toto také zahrnuje všechny činnosti, při nichž zpracování údajů tvoří neoddělitelnou součást činnosti správce nebo zpracovatele.

Význam „rozsáhlosti" je důležité téma, protože i malá advokátní kancelář může mít případy s velkým množstvím údajů. Lze ale snadno tvrdit, na základě bodu odůvodnění 91, že se tento požadavek nebude vztahovat na advokáty vykonávající advokacii samostatně.

Povinnosti a úkoly DPO

GDPR ukládá DPO významné povinnosti, např. monitorování souladu s tímto nařízením, dalšími ustanoveními Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele, dále rozsah odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a provádění souvisejících auditů. DPO rovněž působí jako kontaktní místo pro orgány pro ochranu údajů.

Určený DPO, ať již jde o zaměstnance dané advokátní praxe, nebo ne, by měl mít odborné znalosti předpisů v oblasti ochrany osobních údajů a být schopen plnit všechny úkoly na základě čl. 39 GDPR, např. uchovávání dokumentace veškerých operací zpracování, sledování jejich provádění a školení pracovníků, provádění auditů apod.

Advokáti působící jako DPO

Mohlo by se zdát, že nejvhodnější osobou pro jmenování DPO by měl být advokát, ale je třeba mít na paměti, že s ohledem na rozmanitost povinností vyžadovaných tímto nařízením bude osoba jmenovaná jako DPO vyžadovat více než samotnou právní kvalifikaci.

Asimilace těchto dvou funkcí (advokát/DPO) a riziko záměny mezi těmito funkcemi jsou klíčovým bodem pro jakéhokoli advokáta, který by mohl být jmenován DPO na žádost klienta. Advokát v této pozici může zjistit, že bude muset alternovat mezi funkcí DPO a funkcí advokáta vykonávajícího regulované povolání. Advokát v postavení DPO bude muset zajistit nezávislost a zabránit střetu zájmů, zejména střetům, které mohou plynout z toho, že je zároveň kontaktní osobou pro orgán pro ochranu údajů (což je role, která zahrnuje ohlašovací povinnost úřadu, i když je to proti zájmům správce nebo zpracovatele), zatímco má rovněž povinnost zastupovat zájmy klienta v plném rozsahu povoleném zákonem. **Vzhledem k tomuto možnému střetu zájmů mohou advokátní komory advokátům doporučit, aby tuto odpovědnost DPO pro externího klienta na sebe vzali, pouze pokud nepůsobili jako advokáti v záležitostech, které mohou spadat do oblasti působnosti DPO, ani nebudou po dobu výkonu funkce DPO působit jako advokáti v záležitostech, jichž se účastnili jako DPO.**

Posouzení vlivu

Pokud je, dle čl. 35, pravděpodobné, že určitý druh zpracování (zejména při využití nových technologií, s přihlédnutím k účelům zpracování atd.) bude mít za následek vysoké riziko pro práva a svobody fyzických osob, včetně jakéhokoli rozsáhlého zpracování zvláštních kategorií údajů, správce je před zpracováním povinen provést posouzení vlivu.

Je důležité si uvědomit, že v bodu odůvodnění 91 je vysvětleno, že zpracování

2 http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d57637cb18820e4ceb913ecf71af33028d.e34KaxiLc3qMb40Rch0SaxuTahn0?text=&docid=152065&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=1115616.

3 Tj. „[...] údaje, 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."

osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů klientů jednotlivými právníky. Toto je výjimka, která jednoznačně platí pro advokáty vykonávající profesi samostatně, ale **i u malé advokátní praxe může být vyžadováno, aby příležitostně tato posouzení prováděla**.

Problém je, že podle stávajících standardů (jež nejsou stanoveny pro konkrétní odvětví) mohou být standardy rámců posouzení vlivu na ochranu osobních údajů pro malé praxe neúnosné. Např. i pouhý požadavek, aby správci údajů identifikovali software a hardware používané pro zpracování osobních údajů, může být určitými úřady vykládán jako požadavek na zavedení systému řízení konfigurací a změn. **Obecně nejsou malé praxe s několika zaměstnanci (které jsou ale nad hranicí „samostatného advokáta") v pozici, aby ve všech případech dodržely tyto požadavky v úzkém slova smyslu.** Systém řízení změn by vyžadoval kontrolovaný a rozvinutý systém provozu jejich IT systému, což obvykle není pro praxe této velikosti charakteristické. (Je velmi rozdílné mít hrubý přehled o IT komponentech, které daná praxe má, a mezi fungující a kontrolovanou správou konfigurací a změn.)

Pokyny WP29 ohledně pověřenců pro ochranu osobních údajů (DPO) přijaté 13. 12. 2016 ani aktuálně dostupný návrh pokynů WP29 ohledně posouzení vlivu na ochranu osobních údajů (DPIA) bohužel v tomto ohledu další informace neposkytují. Pokud jde o bod odůvodnění 91, poznámka pod čarou č. 14 pokynů ohledně DPO poukazuje na to, že vše mezi zpracováním samostatným advokátem a zpracováním údajů celé země je šedá zóna. Tato vágnost bude nevyhnutelně vést k různým výkladům.[4]

I když jde o novou zátěž pro advokátní praxe, nařízení si slibuje to, že advokátní praxe budou moci identifikovat a řešit rizika, která by jinak nebyla zjištěna, a zabránit porušení zabezpečení, k nimž by jinak došlo.

V porovnání s oznámením o porušení zabezpečení osobních údajů **neexistuje jasná regulatorní historie ani pokyny, jak by v advokátních kancelářích nebo u jiných podobných profesionálů měla být posouzení vlivu prováděna**.

V současné době jsou posouzení vlivu na ochranu osobních údajů rozmanitá co do obsahu i metod a jsou většinou populární v zemích s tradicí angloamerického práva.[5] V Evropě vydal v roce 2014 úřad informačního komisaře Spojeného království dokument *„Privacy Impact Assessment Code of Practice" (Kodex posuzování vlivu na soukromí)*[6] a francouzský orgán pro ochranu údajů (CNIL) vydal návod k posuzování vlivu na soukromí v roce 2015.[7] Rovněž Evropská komise vydala doporučení vyzývající k posuzování vlivu v souvislosti s čipy RFID[8] *(radio frequency identifier chips)*, které vyústilo v dohodu v daném odvětví ze dne 12. 1. 2011, *„Privacy and Data Protection Impact Assessment Framework for RFID Applications" (Rámec pro posuzování vlivů na soukromí a ochranu údajů u aplikací RFID).* Tento rámec byl schválen WP29 a sloužil rovněž jako vzor pro podobnou „vzorovou" iniciativu u inteligentních měřičů.[9]

Tato doporučení jsou bohužel konkrétní pro oblast, jíž se týkají, a pravděpodobně je nebude možné použít jako zdroj praktických pokynů pro posuzování vlivu advokáty nebo podobnými profesionály v kontextu oznamování porušení zabezpečení osobních údajů.

Advokátům, které zajímá obecné pozadí posouzení vlivu na soukromí, mohou pomoci výsledky studie posuzování vlivu na soukromí financované Komisí (Rámec posouzení vlivu na soukromí u ochrany osobních údajů a práv na soukromí).[10]

Souhrnně lze říci, že **i když se samo nařízení zabývá některými aspekty posouzení vlivu detailně, samotné praktické požadavky nejsou dosud známy**. Očekává se, že dozorové úřady a výše uvedená Rada poskytnou další pokyny u chybějících detailů, např. ve vztahu k druhu operací zpracování, v nichž mohou být tato posouzení vlivu vyžadována.

Přenositelnost údajů

Subjekty údajů mají právo od správce obdržet kopii osobních údajů, které se na ně vztahují a které jsou nebo byly zpracovány. Čl. 20 nařízení vyžaduje, aby byly tyto údaje předány ve **strukturovaném, běžně používaném a strojově čitelném formátu**.

Podle pokynů WP29 ohledně práva na „přenositelnost údajů" jsou pojmy „strukturovaný", „běžně používaný" a „strojově čitelný" souborem minimálních požadavků, které by měly usnadnit interoperabilitu formátu údajů poskytovaných správcem údajů. Pokyny WP29 rovněž uvádějí, že vzhledem k široké škále možných typů údajů, které může správce údajů zpracovávat, GDPR neukládá konkrétní doporučení pro formát těchto osobních údajů, jež mají být poskytnuty.

I když je požadavek na běžně používaný a strojově čitelný formát snadno splnitelný, otázka „strukturovanosti" může být značným problémem. Dokumenty, které advokáti používají, mají obvykle nestrukturovaný obsah. Pro předávání úplných soudních spisů nebo případů ve strukturovaném formátu neexistuje všeobecně přijímaný formát.

Všichni advokáti vědí, jak předávat spisy advokátním kancelářím nově určeným bývalými klienty, ale někdy je přesný formát a struktura tohoto předání již v oblasti, kde mohou mezi advokáty vzniknout spory. **V budoucnosti tento problém může vyžadovat další regulaci advokátními komorami.**

Schopnost sledovat příjemce osobních údajů

Správci údajů mají povinnost být schopni sledovat příjemce osobních údajů patřících konkrétní osobě (přinejmenším jméno a kontaktní údaje pro elektronickou komunikaci). Toto je opět povinnost, kterou by řada advokátních praxí splnila, pouze pokud by ve svých IT systémech provedla určité změny. ✤

4 Vzhledem k tomu, že v době psaní tohoto dokumentu pracovní skupina zřízená podle čl. 29 stále shromažďuje komentáře zúčastněných subjektů k pokynům ohledně posouzení vlivu na ochranu osobních údajů (DPIA), revidovaná a konečná verze by mohla být publikována v průběhu roku 2017 a mohla by obsahovat objasnění toho, co je u činností zpracování „rozsáhlé".

5 Za základy posouzení vlivu na soukromí se považují posouzení dopadu na životní prostředí původně z USA, viz část D1 dokumentu PIAF na http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

6 Viz https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

7 Viz https://www.cnil.fr/fr/node/15798.

8 Viz doporučení Komise 2009/387/ES na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:CS:PDF.

9 Viz doporučení Komise 2012/148/EU a jeho schválení WP29 na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_cs.pdf.

10 http://www.piafproject.eu/About%20PIAF.html.