

PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

16/EN
WP 243 rev.01

Vodítka k pověřencům pro ochranu osobních údajů

Schváleno dne 13. prosince 2016

Revize schválena 5. dubna 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytl Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

**PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE
ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ**

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice a

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

Obsah

1 ÚVOD

2 JMENOVÁNÍ POVĚŘENCE

2.1. POVINNÉ JMENOVÁNÍ

2.1.1 *Veřejný orgán nebo veřejný subjekt*

2.1.2 *Hlavní činnosti*

2.1.3 *Rozsáhlé zpracování*

2.1.4 *Pravidelné a systematické monitorování*

2.1.5 *Zvláštní kategorie údajů a údaje týkající se rozsudků v trestních věcech a trestných činů*

2.2. POVĚŘENEC ZPRACOVATELE

2.3. JMENOVÁNÍ JEDINÉHO POVĚŘENCE PRO VÍCE ORGANIZACÍ

2.4. DOSAŽITELNOST A SÍDLO POVĚŘENCE

2.5. ODBORNÉ ZNALOSTI A SCHOPNOSTI POVĚŘENCE

2.6. ZVEŘEJŇOVÁNÍ A SDĚLOVÁNÍ KONTAKTNÍCH ÚDAJŮ POVĚŘENCE

3 POSTAVENÍ POVĚŘENCE

3.1. ZAPOJENÍ POVĚŘENCE DO VEŠKERÝCH ZÁLEŽITOSTÍ SOUVISEJÍCÍCH S OCHRANOU OSOBNÍCH ÚDAJŮ

3.2. NEZBYTNÉ ZDROJE

3.3. POKYNY A PLNĚNÍ POVINNOSTÍ A ÚKOLŮ NEZÁVISLÝM ZPŮSOBEM

3.4. PROPUŠTĚNÍ NEBO SANKCIONOVÁNÍ POVĚŘENCE V SOUVISLOSTI S PLNĚNÍM JEHO ÚKOLŮ

3.5. STŘET ZÁJMŮ

4 ÚKOLY POVĚŘENCE

4.1. MONITOROVÁNÍ SOULADU S OBECNÝM NAŘÍZENÍM

4.2. ROLE POVĚŘENCE PŘI POSUZOVÁNÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

4.3. SPOLUPRÁCE S DOZOROVÝM ÚŘADEM A PŮSOBENÍ JAKO KONTAKTNÍ MÍSTO

4.4. PŘÍSTUP ZALOŽENÝ NA RIZIKU

4.5. ROLE POVĚŘENCE PŘI VEDENÍ ZÁZNAMŮ

5 PŘÍLOHA – VODÍTKA K POVĚŘENCŮM: CO POTŘEBUJETE VĚDĚT

JMENOVÁNÍ POVĚŘENCE

1. KTERÉ ORGANIZACE MUSÍ JMENOVAT POVĚŘENCE?

2. CO SE ROZUMÍ POJMEM „HLAVNÍ ČINNOSTI“?

3. CO ZNAMENÁ „ROZSÁHLÝ“?

4. CO ZNAMENÁ „PRAVIDELNÉ A SYSTEMATICKÉ MONITOROVÁNÍ“?

5. MOHOU ORGANIZACE JMENOVAT POVĚŘENCE SPOLEČNĚ? POKUD ANO, ZA JAKÝCH PODMÍNEK?

6. KDE MÁ POVĚŘENEC SÍDLIT?

7. LZE JMENOVAT EXTERNÍHO POVĚŘENCE?

8. JAKÉ PROFESNÍ KVALITY BY POVĚŘENEC MĚL MÍT?

POSTAVENÍ POVĚŘENCE

9. JAKÉ ZDROJE BY SPRÁVCE NEBO ZPRACOVATEL MĚL POVĚŘENCI POSKYTNOUT PRO PLNĚNÍ ÚKOLŮ?

10. JAKÉ JSOU ZÁRUKY UMOŽŇUJÍCÍ POVĚŘENCI PLNIT ÚKOLY NEZÁVISLÝM ZPŮSOBEM? CO ZNAMENÁ „KONFLIKT ZÁJMŮ“?

ÚKOLY POVĚŘENCE

11. CO ZNAMENÁ „MONITOROVÁNÍ SOULADU“?

12. JE POVĚŘENEC OSOBNĚ ODPOVĚDNÝ V PŘÍPADĚ NESOULADU S POŽADAVKY OHLEDNĚ OCHRANY OSOBNÍCH ÚDAJŮ?

13. JAKÁ JE ROLE POVĚŘENCE V SOUVISLOSTI S POSUDKY VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ A SE ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ?

1 Úvod

Obecné nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“)¹, které nabude účinnosti 25. května 2018, poskytuje modernizovaný, na zásadě odpovědnosti založený rámec pro dodržování souladu se zásadami ochrany osobních údajů v Evropě. Pověřenci pro ochranu osobních údajů (dále jen „pověřenci“) budou hrát v mnoha organizacích významnou roli, napomáhaje zajišťovat soulad s ustanoveními Obecného nařízení.

Někteří správci a zpracovatelé musí podle Obecného nařízení povinně jmenovat pověřence². Je to případ všech orgánů veřejné moci a veřejných subjektů (bez ohledu na to, jaká data zpracovávají) a dalších organizací, které – jako hlavní činnost – systematicky a rozsáhle monitorují jednotlivce nebo rozsáhle zpracovávají zvláštní kategorie údajů.

I v případech, kdy Obecné nařízení konkrétně nevyžaduje jmenování pověřence, mohou organizace dospět k závěru, že dobrovolné ustavení pověřence může být užitečné. Pracovní skupina podle článku 29 (dále jen „WP29“) takové dobrovolné snahy podporuje.

Koncept pověřence není nový. Přestože směrnice 95/46/ES³ nepožadovala, aby organizace jmenovaly pověřence, rozvinula se během let tato praxe v několika členských státech.

Před přijetím Obecného nařízení argumentovala WP29, že pověřenec je úhelným kamenem zásady odpovědnosti a jeho jmenování může usnadnit dosažení právního souladu a stát se i konkurenční výhodou firmy.⁴ Vedle pomoci při dosahování právní shody uplatněním nástrojů pro zajištění odpovědnosti (pomoc při posuzování vlivu na ochranu osobních údajů a provádění nebo usnadnění auditů), vystupují pověřenci jako prostředníci mezi zainteresovanými stranami (např. orgány dozoru, subjekty údajů a odděleními v rámci organizace).

Pověřenci nenesou osobní odpovědnost za nedodržování Obecného nařízení. Toto nařízení jasně stanoví, že jsou to správci nebo zpracovatelé, kteří musí zajistit a být schopni doložit, že zpracování je prováděno v souladu s jeho ustanoveními (Článek 24, odst. 1). Právní soulad v oblasti ochrany dat je odpovědností správce nebo zpracovatele.

Správce a zpracovatel mají také klíčovou roli při vytváření podmínek pověřencovi pro účinné plnění jeho úkolů. Jmenování je první krok, avšak pověřenec musí mít dostatečnou samostatnost a zdroje pro efektivní výkon funkce.

Obecné nařízení chápe pověřence jako klíčového hráče v novém systému správy dat a stanoví podmínky jeho jmenování, pracovního zařazení jakož i jeho úkoly. Cílem těchto pokynů je objasnit příslušná ustanovení Obecného nařízení a pomoci tak správcům a zpracovatelům vyrovnat se s právními předpisy a ovšem poskytnout také asistenci pověřencům při plnění jejich role. Pokyny také poskytují praktická doporučení, vycházejí ze zkušeností některých členských

¹ Nařízení (EU) 2016/679 Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (Úř. věst. L 119, 4.5.2016).

² Jmenovat pověřence jsou povinny také příslušné orgány ve smyslu článku 32 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, str. 89-131) a národní legislativy, která tuto směrnici implementuje. Tyto pokyny se sice zaměřují na pověřence podle Obecného nařízení, jsou však relevantní, vzhledem k obdobným ustanovením, i pro pověřence podle směrnice 2016/680.

³ Směrnice 95/46/ES Evropského parlamentu a Rady ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, str.31).

⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

států. WP29 bude sledovat naplňování těchto pokynů a může je v případě potřeby doplnit o další podrobnosti.

2 Jmenování pověřence

2.1. Povinné jmenování

Obecné nařízení v článku 37, odst. 1 požaduje jmenovat pověřence ve třech konkrétních případech:⁵

- a) pokud zpracování provádí orgán veřejné moci či veřejný subjekt⁶
- b) pokud hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo
- c) pokud hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů⁷ nebo⁸ osobních údajů týkajících se rozsudků v trestních věcech a trestných činů⁹

V dalším textu poskytuje WP29 rady ohledně kritérií a terminologie v článku 37, odst. 1.

Není-li zřejmé, že organizace nemusí pověřence jmenovat, doporučuje WP29 správcům a zpracovatelům, aby doložili interní analýzou, zda je nebo není nutné pověřence ustavit a mohli tak prokázat, že řádně zohlednili důležité faktory.¹⁰ Tato analýza bude součástí dokumentace pořízené podle zásady odpovědnosti. Dozorový úřad o ni může požádat a měla by být podle potřeby aktualizována, například když správce nebo zpracovatel začne vykonávat nové činnosti nebo poskytovat nové služby, jež mohou spadat mezi případy uvedené v článku 37 odst. 1.

Ustanoví-li organizace pověřence dobrovolně, podléhá jeho jmenování, postavení a úkoly článkům 37 až 39 stejně jako kdyby jmenování bylo povinné.

Nic nebrání organizaci, která není ze zákona povinná jmenovat pověřence a ani ho nechce jmenovat dobrovolně, přesto najmout zaměstnance nebo externí konzultanty pro úkoly související s ochranou osobních údajů. V takovém případě je nutné zajistit, aby nedocházelo k nedorozumění ohledně jejich funkce, postavení a úkolů. Mělo by tedy být uvnitř společnosti i navenek vůči orgánům dozoru, subjektům údajů a široké veřejnosti jasně sděleno, že takový pracovník nebo konzultant není v postavení pověřence pro ochranu osobních údajů.¹¹

Pověřenec, povinný nebo dobrovolný, je jmenován pro veškeré operace zpracování prováděné správcem nebo zpracovatelem.

2.1.1 Veřejný orgán nebo veřejný subjekt

⁵ Podle článku 37, odst. 4 může Unie nebo členské státy zákonem vyžadovat jmenování pověřence i v jiných případech.

⁶ S výjimkou soudů jednajících v rámci svých soudních pravomocí. Viz článek 32 Směrnice (EU) 2016/680.

⁷ Podle článku 9 sem patří osobní údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení či odborovou příslušnost a dále zpracování genetických a biometrických dat za účelem jednoznačné identifikace fyzické osoby, údaje týkající se zdraví nebo údaje o pohlavním životě nebo orientaci fyzické osoby.

⁸ V článku 37, odst. 1, písm. c je použita spojka „a“. Použití „nebo“ namísto „a“ je vysvětleno v kapitole 2.1.5 níže.

⁹ Článek 10.

¹⁰ Viz článek 24, odst. 1.

¹¹ Platí to i pro členy vedení organizace pověřených ochranou soukromí (Chief Privacy Officers) a ostatní odborníky na tuto oblast již dnes působících v některých firmách, kteří nemusí vždy splňovat kritéria Obecného nařízení, například pokud jde o dostupné zdroje nebo záruky nezávislosti a pokud je skutečně nesplňují, nemohou být považováni za pověřence.

Obecné nařízení nevysvětluje, co znamená „veřejný orgán nebo veřejný subjekt“. WP29 se domnívá, že tento pojem by měl být definován národním právem. Veřejnými orgány a subjekty jsou národní, regionální a místní úřady, ale tento koncept podle platného národního práva typicky zahrnuje řadu dalších subjektů řídicích se veřejným právem.¹² V takových případech je jmenování pověřence povinné.

Úkol ve veřejném zájmu a výkon veřejné moci může být plněn¹³ nejenom veřejným orgánem nebo subjektem, ale také jinými fyzickými nebo právními osobami řídicími se veřejným nebo soukromým právem v oblastech specifikovaných národními předpisy členských států, jako je veřejná doprava, zásobování vodou a energiemi, silniční infrastruktura, veřejnoprávní vysílání, veřejné bydlení nebo disciplinární orgány pro vázané profese.

V těchto případech mohou být subjekty údajů v situaci velmi podobné té, kdy jejich data jsou zpracovávána veřejným orgánem nebo subjektem. Zvláště proto, že data mohou být zpracovávána pro podobné účely, přičemž jednotlivci často mají malý nebo nemají žádný vliv na to, zda a jak budou jejich data zpracovávána a mohou tedy požadovat dodatečnou ochranu, jakou může přinést jmenování pověřence.

Ačkoliv v těchto případech to není povinné, WP29 doporučuje jako osvědčený postup, aby soukromé organizace vykonávající úkol ve veřejném zájmu zadání nebo funkci orgánu veřejné moci jmenovaly pověřence. Činnost tohoto pověřence se vztahuje na veškeré operace zpracování včetně těch, které nesouvisí s plněním úkolu ve veřejném zájmu nebo úřední povinnosti (např. správa databáze zaměstnanců).

2.1.2 Hlavní činnosti

Obecné nařízení v článku 37, odst. 1, písm. b) a c) pojednává o „*hlavních činnostech správce nebo zpracovatele*“. Recitál 97 upřesňuje, že hlavní činnosti správce souvisejí „*s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost*“. „*Hlavní činnosti*“ mohou být chápány jako klíčové operace nezbytné k dosažení cílů správce nebo zpracovatele.

„Hlavní činnosti“ by však neměly být interpretovány způsobem vydělujícím aktivity, při nichž zpracování dat tvoří nedílnou součást činnosti správce nebo zpracovatele. Například, hlavní činnost nemocnice je poskytovat zdravotní péči. Nemocnice však nemůže poskytovat zdravotní péči bezpečně a účinně bez zpracování zdravotních dat, jako jsou zdravotní záznamy o pacientovi. Zpracování těchto údajů by tedy mělo být považováno za jednu z hlavních činností a nemocnice proto musí jmenovat pověřence.

Jiným příkladem je soukromá bezpečnostní agentura vykonávající dohled v určitém počtu soukromých nákupních center a veřejných míst. Hlídkání je hlavní činností firmy, je ovšem neoddělitelně spjata se zpracováním osobních údajů. Tato agentura musí proto jmenovat pověřence.

Na druhé straně, všechny organizace provádějí určité činnosti, například vyplácení zaměstnanců nebo poskytování standardní podpory informační a komunikační techniky. To jsou příklady potřebných funkcí podporujících hlavní činnost nebo podnikání organizace. Byť nutné nebo důležité, jsou tyto aktivity obvykle brány spíše jako pomocné funkce než hlavní činnost.

2.1.3 Rozsáhlé zpracování

¹² Viz například definice pojmů „subjekt veřejného zájmu“ a „veřejnoprávní subjekt“ v článku 2, odst. 1 a 2 směrnice 2003/98/ES Evropského parlamentu a Rady ze dne 17. listopadu 2003 o opakovaném použití informací veřejného sektoru (Úř. věst. L 345, 31.12.1995, str.90).

¹³ Článek 6, odst. 1, písm. e.

Podle článku 37, odst. 1, písm. b) a c) musí být zpracování osobních údajů prováděno ve velkém rozsahu, aby to vyvolalo povinnost jmenovat pověřence. Obecné nařízení nedefinuje, co činí zpracování rozsáhlým, určitý návod poskytuje recitál 91.¹⁴

Vskutku není možné uvést nějaké přesné, pro všechny situace použitelné, číslo udávající množství zpracovávaných dat nebo počet dotčených jednotlivců. Není vyloučeno, že se časem vyvine standardní praxe jak přesněji určit a/nebo množstevně vyjádřit pojem „rozsáhlý“ ve vztahu k určitým typům obvyklých činností zpracování. WP29 plánuje přispět k tomuto vývoji sdílením a uveřejňováním příkladů relevantních ukazatelů signalizujících nutnost jmenovat pověřence.

WP29 každopádně doporučuje vzít při určování rozsáhlosti zpracování v úvahu následující faktory:

- počet dotčených subjektů údajů – vyjádřený buď konkrétním číslem, nebo podílem na relevantní populaci
- objem dat a/nebo rozsah různých datových položek
- doba trvání nebo nepřetržitost zpracování
- územní rozsah zpracování

Příklady rozsáhlého zpracování:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové průkazky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů jednotlivým právníkem

2.1.4 Pravidelné a systematické monitorování

Pojem pravidelného a systematického monitorování subjektů údajů není v Obecném nařízení definován, avšak koncept „monitorování chování subjektů údajů“ je zmíněn v recitálu 24¹⁵ a jasně zahrnuje všechny formy sledování a profilování na internetu, i pro účely behaviorální reklamy.

¹⁴ Jde především o citaci „rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko“. Recitál na druhé straně konkrétně stanoví, že „zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo právníky“. Je třeba si uvědomit, že příklady uvedené v recitálu představují krajní body na opačných koncích pomyslné stupnice (zpracování jednotlivým lékařem v protikladu k zpracování osobních údajů za celou zemi nebo Evropu) a mezi nimi leží velká šedá zóna. Také je třeba mít na paměti, že tento recitál se týká posouzení vlivu na ochranu osobních údajů. Některé prvky mohou tedy být specifické v tomto kontextu a nemusí nutně platit stejným způsobem pro jmenování pověřenců.

¹⁵ „Aby se určilo, zda může být činnost zpracování považována za monitorování chování subjektů údajů, mělo by být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, která se jí týkají, nebo za účelem analýzy či odhadu jejich osobních preferencí, postojů a chování.“

Pojem sledování není však omezen pouze na prostředí online, přičemž sledování na internetu by mělo být bráno jen jako jeden z příkladů monitorování chování subjektů údajů.¹⁶

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanoveném čase
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů: provozování telekomunikační sítě; poskytování telekomunikačních služeb; cílení internetové reklamy pomocí e-mailu, marketing řízený daty, profilování a bodování (skórování) pro účely posouzení rizik (např. pro účely hodnocení úvěrového rizika, stanovení výše pojistného, předcházení podvodům, odhalování praní špinavých peněz), sledování polohy, například u mobilních aplikací, věrnostní programy; behaviorální reklama, sledování zdravého životního stylu, tělesné kondice a zdravotních dat pomocí na těle nositelných zařízení, kamerové systémy; propojená zařízení, např. chytré měřiče, chytrá auta, inteligentní domy, atd.

2.1.5 Zvláštní kategorie údajů a údaje týkající se rozsudků v trestních věcech a trestných činů

Článek 37, odst. 1, písm. c) se vztahuje na zpracování zvláštních kategorií údajů podle článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů podle článku 10. I když je v ustanovení užitá spojka „a“, není důvod tato dvě kritéria aplikovat zároveň. Text by proto měl být chápán, jako kdyby v něm stálo „nebo“.

2.2. Pověřenec zpracovatele

Článek 37 platí pro správce¹⁷ i zpracovatele¹⁸ pokud jde o jmenování pověřence. V některých případech může pověřence ustanovit jen správce nebo jen zpracovatel, podle toho, kdo z nich splňuje kritéria povinného jmenování. V jiných případech musí pověřence jmenovat správce i zpracovatel (oba by pak měli vzájemně spolupracovat).

Je důležité vyzdvihnout, že i pokud správce splňuje kritéria povinného jmenování, jeho zpracovatel nemusí nutně pověřence jmenovat. Může to však být dobrou praxí.

Příklady:

- Malý rodinný podnik prodávající domácí spotřebiče v jediném městě využívá služeb zpracovatele, jehož hlavní činností je analýza webových stránek a pomoc s cílenou reklamou a marketingem. Činnost rodinného podniku ani jeho zákazníci nezavdávají důvod k rozsáhlému zpracování dat vzhledem k jejich malému počtu a poměrně omezeným aktivitám. Zato zpracovatel, máje dohromady mnoho takových klientů jako

¹⁶ Recitál 24 se zaměřuje na extraterritoriální uplatnění Obecného nařízení. Navíc je zde rozdíl mezi formulací „monitorování jejich chování“ (článek 3, odst. 2, písm. b) a „pravidelné a systematické monitorování subjektů údajů“ (článek 37, odst. 1, písm. b), který by mohl vést k domněnce, že jde o dva odlišné pojmy.

¹⁷ Správce je definován v článku 4, odst. 7 jako osoba nebo orgán, který určuje účely a prostředky zpracování.

¹⁸ Zpracovatel je definován v článku 4, odst. 8 jako osoba nebo orgán, který zpracovává osobní údaje pro správce.

zmíněná malá firma, rozsáhlé zpracování provádí. Musí tedy jmenovat pověřence podle článku 37, odst. 1, písm. b). Naproti tomu tento rodinný podnik povinnosti jmenovat pověřence nepodléhá.

- Středně velký výrobce obkladaček zajišťuje ochranu zdraví zaměstnanců smluvně přes externí firmu, která má velký počet podobných klientů. Tato firma (zpracovatel) musí jmenovat pověřence podle článku 37, odst. 1, písm. c) za předpokladu, že se jedná o rozsáhlé zpracování. Výrobce však povinnosti jmenovat pověřence nutně nepodléhá.

Pověřenec jmenovaný zpracovatelem dohlíží rovněž na činnosti, které zpracovatelská organizace vykonává pro sebe jako správce (např. personalistika, IT, logistika).

2.3. Jmenování jediného pověřence pro více organizací

Článek 37, odst. 2 dovoluje skupině podniků jmenovat jediného pověřence, pokud bude „*snadno dosažitelný z každého podniku*“. Pojem dosažitelnosti se vztahuje k úkolům pověřence jako kontaktního bodu pro subjekty údajů¹⁹, orgány dozoru²⁰, ale také uvnitř organizace, vzhledem k tomu, že jedním z úkolů pověřence je „*poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení*“.²¹

K zajištění dostupnosti pověřence, ať interního nebo externího, je důležité, aby byly k dispozici jeho kontaktní údaje v souladu s požadavky Obecného nařízení.²²

Pověřenec, pokud nutno s pomocí týmu, musí být schopen účinně komunikovat se subjekty údajů²³ a spolupracovat²⁴ s příslušným dozorovým úřadem. Také to znamená, že komunikovat se musí v jazyce nebo jazycích užívaných dotčenými orgány dozoru a subjekty údajů. Dosažitelnost pověřence (fyzicky na stejném pracovišti jako zaměstnanci, přes horkou linku nebo bezpečné komunikační prostředky) je zásadní pro zajištění, že subjekty údajů budou schopny pověřence kontaktovat.

Podle článku 37, odst. 3, může jediný pověřenec být jmenován pro několik orgánů veřejné moci či veřejných subjektů při zohlednění jejich organizační struktury a velikosti. Totéž platí pro zdroje a komunikaci. V odpovědnosti pověřence jsou rozmanité úkoly, proto musí správce nebo zpracovatel zajistit, aby jediný pověřenec, s pomocí týmu, bude-li nezbytné, je zvládnul plnit efektivně i přesto, že byl jmenován pro několik orgánů veřejné moci nebo veřejných subjektů.

2.4. Dosažitelnost a sídlo pověřence

Pověřenec by měl být, podle Oddílu 4 Obecného nařízení, skutečně dostupný.

WP29 doporučuje jako obecné pravidlo, aby v zájmu dosažitelnosti pověřenec sídlil v Evropské unii, bez ohledu, zda správce nebo zpracovatel je v Evropské unii usazen.

¹⁹ Článek 38, odst. 4: „*Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení*“.

²⁰ Článek 39, odst. 1, písm. e): působí jako „*kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci*“.

²¹ Článek 39, odst. 1, písm. a).

²² Viz také oddíl 2.6. níže.

²³ Článek 12, odst. 1: „*Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti*“.

²⁴ Článek 39, odst. 1, písm. d): „*spolupráce s dozorovým úřadem*“

Nelze však vyloučit, že v některých situacích, kdy správce nebo zpracovatel nebude mít provozovnu v Evropské unii²⁵, může pověřenec vyvíjet činnost účinněji, bude-li sídlit mimo EU.

2.5. Odborné znalosti a schopnosti pověřence

Článek 37, odst. 5 stanoví, že pověřenec „*musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů a své schopnosti plnit úkoly stanovené v článku 39*“. Recitál 97 říká, že potřebná úroveň odborných znalostí by měla být určena podle prováděných operací zpracování a podle ochrany požadované pro zpracovávané osobní údaje.

- **Úroveň odborných znalostí**

Požadovaná úroveň odborných znalostí není přesně definována, musí však být úměrná citlivosti, složitosti a množství dat, které organizace zpracovává. Například tam, kde činnost zpracování dat je obzvláště složitá, nebo zahrnuje velké množství dat, bude zřejmě pověřenec potřebovat vyšší úroveň znalostí a větší podporu. Je také rozdíl, zda organizace předává osobní údaje mimo Evropskou unii systematicky nebo příležitostně. Pověřenec by tedy měl být vybrán pečlivě s náležitým zvážením specifických otázek ochrany dat, které organizace řeší.

- **Profesní kvality**

Ačkoliv článek 37, odst. 5 neupřesňuje, jaké profesní kvality by při jmenování pověřence měly být zváženy, podstatné musí být vědomosti z oblasti národní a evropské legislativy a praxe v oboru ochrany osobních údajů a důkladná znalost Obecného nařízení. Prospěšné by bylo, kdyby dozorné úřady propagovaly náležité a pravidelné školení pověřenců.

Užitečná je znalost oboru podnikání a chodu organizace, která je správcem. Pověřenec by také měl mít dobrou znalost prováděných operací zpracování, stejně jako informačních systémů, bezpečnosti dat a správcových potřeb v oblasti ochrany osobních údajů.

V případě orgánu veřejné moci nebo veřejného subjektu by pověřenec měl dobře znát také administrativní pravidla a postupy dané organizace.

- **Schopnost plnit úkoly**

Schopnost plnit úkoly přináležící pověřenci by měla být vykládána jednak ve vztahu k jeho osobním kvalitám a znalostem, ale také s ohledem na jeho postavení v organizaci. Osobní kvality by měly zahrnovat například integritu a vysokou úroveň profesionální etiky. Pověřencův prvotní zájem by měl být soulad s Obecným nařízením. Pověřenec hraje klíčovou roli při rozvoji kultury ochrany dat uvnitř organizace a pomáhá zavádět základní prvky Obecného nařízení, jako jsou zásady zpracování dat²⁶, práva subjektu údajů²⁷, záměrná a standardní ochrana osobních údajů²⁸, záznamy o činnostech zpracování²⁹, zabezpečení zpracování³⁰ a ohlašování a oznamování případů porušení zabezpečení ochrany osobních údajů³¹.

- **Pověřenec na smlouvu o poskytování služeb**

²⁵ Viz článek 3 Obecného nařízení o místní působnosti

²⁶ Kapitola II.

²⁷ Kapitola III.

²⁸ Článek 25.

²⁹ Článek 30.

³⁰ Článek 32.

³¹ Články 33 a 34.

Funkci pověřence je možné vykonávat na základě smlouvy o poskytování služeb uzavřené mezi jednotlivcem nebo externí organizací (jinou, než organizace správce nebo zpracovatele). V posledně jmenovaném případě je důležité, aby každý pracovník organizace vykonávající funkci pověřence splňoval všechny platné požadavky Oddílu 4 Obecného nařízení (například je nutné, aby nikdo nebyl ve střetu zájmů). Stejně tak je důležité, aby každý takový pracovník byl chráněn ustanoveními Obecného nařízení (například smlouva o poskytování služeb nemá být nespravedlivě vypovězena v důsledku činnosti pověřence a také žádný pracovník organizace provádějící úkoly pověřence nemá být nespravedlivě propuštěn). Je také možné kombinovat individuální schopnosti a silné stránky, takže více pracovníků pracujících jako tým může účinněji poskytovat služby svým klientům.

V zájmu právní průhlednosti a dobré organizace, jakož i v zájmu předcházení konfliktům zájmů členů týmu, se doporučuje jasně rozdělit úkoly v pověřencově týmu a určit jednoho pracovníka jako hlavní kontakt a osobu „pověřenou“ péčí o zákazníka. Obecně řečeno, užitečné by bylo vymezit tyto body ve smlouvě o poskytování služeb.

2.6. Zveřejňování a sdělování kontaktních údajů pověřence

Článek 37, odst. 7 Obecného nařízení požaduje, aby správce nebo zpracovatel:

- zveřejnil kontaktní údaje pověřence
- sdělil kontaktní údaje pověřence příslušnému dozorovému úřadu

Tyto požadavky mají zajistit, aby subjekty údajů (uvnitř i mimo organizaci) a dozorové úřady mohly snadno a přímo kontaktovat pověřence, aniž by se musely obracet na jiné složky organizace. Důvěrnost je stejně tak důležitá: zaměstnanci například se mohou zdráhat podat stížnost pověřenci, nebudou-li mít záruku, že jejich sdělení bude bráno jako důvěrné.

Pověřenec je v souvislosti s plněním svých úkolů vázán tajemstvím nebo důvěrností v souladu s právem Unie nebo členského státu (Článek 38, odst. 5).

Kontaktní údaje pověřence by měly obsahovat informaci umožňující subjektům údajů a dozorovým úřadům jednoduchým způsobem ho zastihnout (poštovní adresa, vyhrazené telefonní číslo a/nebo vyhrazená e-mailová adresa). Pro komunikaci s veřejností lze, v odpovídajících případech, poskytnout další způsoby komunikace, například vyhrazenou horkou linku nebo zvláštní kontaktní formulář určený pověřenci na webu organizace.

Článek 37, odst. 7 nevyžaduje uvádět mezi kontaktními údaji jméno pověřence. I když v rámci osvědčených postupů by to bylo vhodné, je na rozhodnutí správce nebo zpracovatele a pověřence, zda je to nezbytné nebo účelné za daných okolností.³²

Je však důležité sdělit jméno pověřence dozorovému úřadu, aby pověřenec mohl fungovat jako kontaktní místo mezi organizací a dozorovým úřadem (Článek 39, odst. 1, písm. e).

WP29 dále doporučuje, aby organizace, v souladu s osvědčenými postupy, sdělily dozorovému úřadu a zaměstnancům jméno a kontaktní údaje pověřence. Jméno a kontaktní údaje pověřence mohou například být interně oznámeny na intranetu organizace, v interním telefonním seznamu a v organigramu.

3. Postavení pověřence

3.1. Zapojení pověřence do veškerých záležitostí souvisejících s ochranou osobních údajů

³² Stojí za zmínku, že článek 33, odst. 3, písm. b), popisující informace, které musí být poskytnuty dozorovému úřadu a subjektům údajů v případě porušení zabezpečení osobních údajů, výslovně vyžaduje, na rozdíl od článku 37, odst. 7, sdělit také jméno (a ne pouze kontaktní údaje) pověřence.

Článek 38 Obecného nařízení stanoví, že správce a zpracovatel zajistí, aby pověřenec „*byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů*“.

Je zásadní, aby pověřenec nebo jeho tým byl zapojen co možná nejdříve do všech záležitostí týkajících se ochrany osobních údajů. V souvislosti s posouzením vlivu na ochranu osobních údajů hovoří Obecné nařízení výslovně o včasném zapojení pověřence a stanovuje, aby si správce vyžádal posudek pověřence, když provádí posouzení vlivu na ochranu osobních údajů.³³ Informování pověřence a konzultace s ním hned na začátku procesu usnadní dosažení shody s Obecným nařízením, podpoří uplatnění přístupu podle zásady záměrné ochrany osobních údajů (Privacy by Design) a mělo by se tak stát standardním postupem v rámci řízení organizace. Důležité je, aby pověřenec byl brán jako diskusní partner uvnitř organizace a byl součástí příslušných pracovních skupin zabývajících se v organizaci zpracováním dat.

Z toho důvodu by organizace například měla zajistit, aby:

- pověřenec byl pravidelně zván na schůze vyššího a středního managementu.
- jeho přítomnost byla doporučena vždy tam, kde se dělají rozhodnutí s dopadem do ochrany osobních údajů. Pověřenec musí včas obdržet všechny podstatné informace, aby mohl poskytnout odpovídající radu.
- stanovisku pověřence byla vždy přiznána patřičná závažnost. Pro případ nesouhlasu doporučuje WP29, jako příklad dobré praxe, zadokumentovat důvody, proč pověřencova rada nebyla následována.
- pověřenec byl bezodkladně konzultován v případě porušení zabezpečení ochrany osobních údajů nebo jiné události.

Správce nebo zpracovatel může, uzná-li za vhodné, vypracovat směrnice nebo programy pro ochranu osobních údajů stanovující, kdy musí být pověřenec konzultován.

3.2. Nezbytné zdroje

Obecné nařízení v článku 38, odst. 2 požaduje, aby organizace podporovaly pověřence „*tím, že mu poskytují zdroje k plnění [těchto] úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí*“. Zvážit je potřeba hlavně tyto aspekty:

- aktivní podpora od vyššího vedení (na úrovni představenstva)
- dostatečný čas pro plnění povinností. To je především důležité v případech, kdy interní pověřenec je jmenován na částečný úvazek nebo tuto funkci vykonává externí pověřenec vedle dalších povinností. Protichůdné priority by mohly vést k zanedbávání povinností pověřence. Zcela zásadní je dostatek času věnovaný úkolům pověřence. Je dobrým zvykem stanovit pevný podíl času vyhrazený pro funkci pověřence, pokud není vykonávána na plný úvazek. Je rovněž dobrým zvykem stanovit čas potřebný k výkonu funkce, náležitou úroveň priority pověřencových povinností a sestavit plán práce pověřence (nebo organizace).
- odpovídající podpora z hlediska peněžních zdrojů, infrastruktury (prostory, vybavení, zařízení) a personálu, pokud je třeba.
- oficiální oznámení o jmenování pověřence všem zaměstnancům, aby bylo zajištěno, že jeho existence a funkce je v organizaci známa.
- nezbytný přístup do jiných útvarů v organizaci, jako personální, právní, IT, bezpečnost, atd., aby měl pověřenec nezbytnou podporu a informace z těchto útvarů
- průběžné školení. Pověřenec musí dostat příležitost udržovat své znalosti v souladu s rozvojem v oblasti ochrany dat. Cílem by mělo být neustálé zvyšování úrovně znalostí a měla by také být podporována účast pověřenců na školeních o ochraně dat a dalších formách profesního rozvoje, jako jsou fóra, semináře, atp.

³³ Článek 35, odst. 2.

- v závislosti na velikosti a struktuře organizace může se ukázat nezbytným sestavit celý tým (pověřenec a jeho personál). V takovém případě by vnitřní struktura týmu a úkoly a odpovědnosti jednotlivých členů měly být jasně stanoveny. Obdobně, pokud funkci pověřence vykonává externí poskytovatel, může skupina lidí pracujících pro tohoto poskytovatele efektivně vykonávat funkci pověřence jako tým, přičemž odpovědnost nese hlavní kontaktní osoba, které byl klient přidělen.

Obecně řečeno, čím složitější a/nebo citlivější jsou operace zpracování, tím více zdrojů musí být pověřenci dáno k dispozici. Tato funkce musí být účinným a dostatečným způsobem zabezpečena zdroji v poměru k prováděnému zpracování.

3.3. Pokyny a plnění povinností a úkolů nezávislým způsobem

Článek 38, odst. 3 stanovuje některé základní záruky napomáhající zajistit, aby pověřenec byl schopen plnit úkoly s dostatečným stupněm samostatnosti v rámci organizace. Od správců a zpracovatelů se zejména vyžaduje zajistit, aby pověřenec „nedostával žádné pokyny týkající se výkonu [jeho] úkolů“. V recitálu 97 je uvedeno, že pověřenci „bez ohledu na to, zda se jedná o zaměstnance správce, by měli být schopni plnit své povinnosti a úkoly nezávislým způsobem“.

To znamená, že při plnění úkolů podle článku 39 nesmí pověřenci dostávat pokyny jak jednat v dané oblasti, například, jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda konzultovat dozorový úřad. Dále jim nesmí být nařizováno přijímat určité názory v záležitostech týkajících se ochrany dat, například konkrétní výklad práva.

Autonomie pověřenců však neznamená, že mají rozhodovací pravomoci přesahující rámec jejich úkolů podle článku 39.

Za dodržení souladu s právními předpisy pro ochranu osobních údajů zůstává odpovědný správce nebo zpracovatel a musí být schopen tento soulad doložit.³⁴ Pokud správce nebo zpracovatel učiní rozhodnutí neslučitelná s Obecným nařízením a s radou pověřence, měl by pověřenec dostat možnost své nesouhlasné stanovisko vysvětlit nejvyššímu vedení a těm, kteří tato rozhodnutí udělali. Článek 38, odst. 1 v tomto ohledu stanoví, že pověřenec „je přímo podřízen vrcholovým řídicím pracovníkům správce nebo zpracovatele“. Taková přímá podřízenost zajišťuje, že se vyšší management (např. představenstvo) dozví o radách a doporučeních pověřence coby součásti jeho poslání informovat a radit správci a zpracovateli. Dalším příkladem přímé podřízenosti je příprava výroční zprávy o činnosti pověřence pro nejvyšší úroveň řízení.

3.4. Propuštění nebo sankcionování pověřence v souvislosti s plněním jeho úkolů

Článek 38, odst. 3 stanoví, že pověřenec „není správcem nebo zpracovatelem propuštěn ani sankcionován v souvislosti s plněním svých úkolů“.

Tento požadavek posiluje samostatné postavení pověřenců a napomáhá zajistit, aby jednali nezávisle a požívali dostatečnou ochranu při plnění svých úkolů v oblasti ochrany dat.

Tresty podle Obecného nařízení jsou zapovězeny, jen pokud jsou uloženy jako následek výkonu povinností pověřence. Například, pověřenec může být názoru, že konkrétní zpracování by mohlo mít za následek vysoké riziko a doporučí správci nebo zpracovateli vypracovat posouzení vlivu na ochranu osobních údajů, ovšem správce nebo zpracovatel nesouhlasí s pověřencovým posudkem. V takové situaci nemůže být pověřenec za své doporučení propuštěn.

Tresty mohou nabývat řady forem a mohou být přímé nebo nepřímé. Mohou například spočívat v zaražení nebo odkladu povýšení, bránění v kariérním postupu či odmítnutí výhod, které jiní

³⁴ Článek 5, odst. 2.

zaměstnanci požívají. Není nutné tyto tresty skutečně dokonat, pouhá jejich hrozba je dostatečná, pokud je užita k potrestání pověřence z důvodů souvisejících s jeho činností.

Podle běžné zásady řízení a jak by se stalo i v případě jiných zaměstnanců nebo smluvních partnerů podléhajících národnímu obchodnímu nebo pracovnímu a trestnímu právu, mohl by pověřenec být legitimně propuštěn z důvodů jiných, než v souvislosti s jeho úkoly pověřence (například v případě krádeže, fyzického, psychického nebo sexuálního obtěžování nebo podobně silně nevhodného chování).

V této souvislosti budiž řečeno, že Obecné nařízení neupřesňuje, jak a kdy může být pověřenec propuštěn nebo nahrazen jinou osobou. Nicméně, čím stabilnější bude pověřencova smlouva a čím více záruk bude mít proti nespravedlivému propuštění, tím je pravděpodobnější, že bude jednat nezávislým způsobem. WP29 proto uvítá ze strany organizací jakékoli snahy v tomto směru.

3.5. Střet zájmů

Článek 38, odst. 6 dovoluje pověřencům „*plnit i jiné úkoly a povinnosti*“. Od organizace to ovšem vyžaduje zabezpečit, aby „*žádné z těchto úkolů a povinností nevedly ke střetu zájmů*“.

Nepřítomnost konfliktu zájmů úzce souvisí s požadavkem nezávislého jednání. Byť pověřenci smějí mít i jiné funkce, mohou jim být svěřeny pouze úkoly a povinnosti, které nezakládají střet zájmů. Především z toho plyne, že pověřenec v organizaci nemůže zastávat pracovní místo, na kterém by stanovoval účely a prostředky zpracování osobních údajů. Vzhledem k organizační struktuře specifické pro každou organizaci, je potřeba tuto otázku řešit případ od případu.

V konfliktním postavení mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování. Konflikt zájmů může také kupříkladu vzniknout, pokud externí pověřenec bude požádán o zastupování správce nebo zpracovatele před soudem v případě týkajícím se ochrany osobních údajů.

V závislosti na činnostech, velikosti a struktuře organizace může správcům a zpracovatelům posloužit jako příklad osvědčeného postupu následující:

- určit pracovní místa neslučitelná s výkonem funkce pověřence
- sestavit vnitřní pravidla k zamezení střetu zájmů
- začlenit do pravidel obecnější vysvětlení střetu zájmů
- prohlásit, že pověřenec není ve střetu zájmů ve vztahu ke své funkci pověřence jako způsob zvyšování povědomí o tomto požadavku
- začlenit do vnitřních pravidel záruky a zajistit, aby oznámení volného místa pověřence nebo smlouvy o poskytování služeb bylo dostatečně přesné a podrobné a tím se zamezilo střetu zájmů. V této souvislosti je dobré mít na paměti, že konflikty zájmů mohou nabývat různých forem podle toho, je-li pověřenec získáván interně nebo externě.

4 Úkoly pověřence

4.1. Monitorování souladu s Obecným nařízením

Článek 39, odst. 1, písm. b) svěřuje pověřencům, kromě jiných povinností, úlohu monitorovat soulad s Obecným nařízením. Recitál 97 dále ve vztahu k pověřencům upřesňuje, že „*měla by*

být správci nebo zpracovateli při monitorování toho, zda je zajištěn vnitřní soulad s tímto [Obecným] nařízením nápomocna osoba s odbornými znalostmi“.

Pověřenec, v rámci svých povinností, může zejména:

- shromažďovat informace za účelem zjišťování zpracovatelských činností
- analyzovat a prověřovat právní soulad zpracovatelských činností
- informovat, radit a vydávat doporučení správci nebo zpracovateli

Monitorování souladu neznamená, že pověřenec je osobně odpovědný za případy nesouladu. Obecné nařízení jasně stanoví, že je to správce, a nikoliv pověřenec, kdo má povinnost, že *„zavede vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto [Obecným] nařízením“.* (Článek 24, odst. 1). Soulad s předpisy o ochraně dat je podniková odpovědnost správce, ne pověřence.

4.2. Role pověřence při posuzování vlivu na ochranu osobních údajů

Podle článku 35, odst. 1 je povinností správce, nikoliv pověřence, provést, pokud je nutné, posouzení vlivu na ochranu osobních údajů (dále jen „posouzení vlivu“). Pověřenec však může sehrát velmi důležitou a užitečnou roli při pomoci správci. Vycházejí z principu záměrné ochrany osobních údajů, obsahuje článek 35, odst. 2 konkrétní požadavek, aby správce *„si vyžádal posudek“* pověřence při provádění posouzení vlivu. Naopak článek 39, odst. 1, písm. c) zadává pověřenci úkol *„poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35“.*

WP29 doporučuje správcům, aby vyžadovali posudek pověřence mimo jiné k následujícím otázkám³⁵:

- zda je nebo není nutné provést posouzení vlivu
- jakou metodiku při zpracování posouzení vlivu použít
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s Obecným nařízením

Nesouhlasí-li správce s posudkem dodaným pověřencem, mělo by v dokumentaci posouzení vlivu být konkrétně odůvodněno, proč posudek nebyl vzat v úvahu³⁶.

WP29 dále doporučuje, aby správce jasně vymezil, například ve smlouvě s pověřencem, ale také v informaci pro zaměstnance i vedení (a pro další zainteresované strany, pokud existují), přesné úkoly pověřence a jejich rozsah, zejména s ohledem na provádění posouzení vlivu.

³⁵ Článek 39, odst. 1 zmiňuje úkoly pověřence a uvádí, že pověřenec má vykonávat *„alespoň“* tyto úkoly. Nic proto nebrání správci, aby pověřenci přidělil i jiné úkoly, než ty, které jsou výslovně uvedeny v článku 39, odst. 1 nebo tyto úkoly upřesnil do většího detailu.

³⁶ Článek 24, odst. 1 stanoví, že *„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.“*

4.3. Spolupráce s dozorovým úřadem a působení jako kontaktní místo

Podle článku 39, odst. 1, písm. d) a e) je úkolem pověřence „*spolupráce s dozorovým úřadem*“ a „*působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci*“.

Tyto úkoly se týkají role pověřence coby nápomocné osoby, jak je zmíněno v úvodu těchto vodítek. Pověřenec jedná jako kontaktní osoba usnadňující dozorovému úřadu přístup k dokumentům a informacím pro výkon úkolů podle článku 57, jakož i pro uplatňování jeho vyšetřovacích, nápravných, povolovacích a poradních pravomocí podle článku 58. Jak již bylo zmíněno, pověřenec je v souvislosti s výkonem svých úkolů vázán tajemstvím a důvěrností v souladu s právem Unie nebo členského státu (Článek 38, odst. 5). Závazek tajemství, resp. důvěrnosti však pověřenci nebrání kontaktovat dozorový orgán se žádostí o radu. Článek 39, odst. 1, písm. e) stanoví, že pověřenec může případně vést konzultace s dozorovým úřadem v jakékoli věci.

4.4. Přístup založený na riziku

Článek 39, odst. 2 říká, že správce „*bere patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování*“.

Tento článek se odvolává na obecnou zásadu organizace práce a na selský rozum, tedy principy, které mohou být důležité v mnoha aspektech každodenní práce pověřence. V podstatě od pověřenců vyžaduje přiřazovat priority svým činnostem a zaměřit úsilí na záležitosti představující zvýšené riziko z hlediska ochrany osobních údajů. To neznamená, že by měli zanedbávat monitorování souladu u operací zpracování, u kterých je srovnatelně menší riziko, pouze upozorňuje, že prvotně by se měli zaměřovat na oblasti s rizikem vyšším.

Tento výběrový a pragmatický přístup by měl pověřencům pomoci při poskytování rad správci ve věci, jakou metodiku použít při provádění posouzení vlivu, které oblasti by měly být předmětem vnitřního nebo externího auditu, jaká interní školení poskytnout zaměstnancům nebo členům vedení zodpovědným za zpracovatelské činnosti a kterým operacím zpracování věnovat více času a zdrojů.

4.5. Role pověřence při vedení záznamů

Článek 30, odst. 1 a 2 stanoví, že správce nebo zpracovatel, nikoliv pověřenec, „*vede záznamy o činnostech zpracování, za něž zodpovídá*“ nebo „*vede záznamy o všech kategoriích činností prováděných pro správce*“.

Pověřenci ve své praxi často vytváří přehledy a vedou registr operací zpracování na základě informací od různých oddělení jejich organizace, zodpovědných za zpracování osobních údajů. Tato praxe se ustálila podle mnoha současných národních zákonů a podle pravidel ochrany dat, kterými se řídí instituce a subjekty EU.³⁷

Článek 39, odst. 1 obsahuje výčet úkolů pověřence v minimálně požadovaném rozsahu. Nic tedy nebrání správci nebo zpracovateli, aby pověřence zaúkolovali vedením záznamů o činnostech zpracování, za něž odpovídají. Takové záznamy by měly být považovány za jeden z nástrojů umožňující pověřenci plnit úkoly spočívající v monitorování souladu a informování a poskytování poradenství správci nebo zpracovateli.

Záznamy vedené podle článku 30 by také měly být brány jako nástroj umožňující správci nebo dozorovému úřadu získat na vyžádání přehled všech činností zpracování osobních údajů

³⁷ Článek 24, odst. 1, písm. d), Nařízení (ES) 45/2001.

v organizaci prováděných. Jsou tedy předpokladem dosažení právního souladu a jako takové i účinným opatřením směrem k odpovědnosti.

5 PŘÍLOHA – VODÍTKA K POVĚŘENCŮM: CO POTŘEBUJETE VĚDĚT

Tato příloha má organizacím poskytnout jednoduché a snadno srozumitelné odpovědi na některé klíčové otázky související se jmenováním pověřence pro ochranu osobních údajů, jak nově požaduje Obecné nařízení o ochraně osobních údajů.

Jmenování pověřence

1 Které organizace musí jmenovat pověřence?

Jmenovat pověřence je povinné, pokud:

- zpracování provádí orgán veřejné moci či veřejný subjekt (bez ohledu na to, jaká data jsou zpracovávána)
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Navíc, právo Unie nebo členských států může vyžadovat jmenování pověřence také v dalších situacích. I v případech, kdy Obecné nařízení nevyžaduje jmenování pověřence, mohou organizace dojít k rozhodnutí, že dobrovolné ustavení pověřence bude užitečné. WP29 takovou dobrovolnou iniciativu podporuje. Pokud organizace jmenuje pověřence dobrovolně, platí pro jeho jmenování, postavení a úkoly stejné požadavky jako kdyby byl ustaven povinně.

Zdroj: Obecné nařízení, článek 37, odst. 1

2 Co se rozumí pojmem „hlavní činnosti“?

Za „hlavní činnosti“ lze považovat klíčové operace směřující k dosažení cílů správce nebo zpracovatele. Sem také patří veškeré aktivity, kde zpracování dat je nedílnou součástí činnosti správce nebo zpracovatele. Například zpracování zdravotních dat, jako jsou zdravotní záznamy pacienta, by mělo být považováno za jednu z hlavních činností a nemocnice tak musí jmenovat pověřence.

Na druhé straně, všechny organizace vykonávají určité podpůrné činnosti, kupříkladu vyplácení zaměstnanců nebo standardní podporu výpočetní a informační techniky. Jde o nezbytné funkce podporující hlavní činnost nebo podnikání organizace. Byť nutné nebo podstatné, jsou tyto činnosti považovány spíše za pomocné funkce, než za klíčovou aktivitu.

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b) a c)

3 Co znamená „rozsáhlý“?

Obecné nařízení nedefinuje pojem rozsáhlé zpracování. WP29 doporučuje při určování, zda zpracování je rozsáhlé, vzít v úvahu zejména následující faktory:

- počet dotčených subjektů údajů – buď v absolutním vyjádření nebo podílem na relevantní populaci
- objem zpracovávaných dat a/nebo rozsah datových položek
- doba trvání nebo nepřetržitost zpracovatelské činnosti
- územní rozsah zpracovatelské činnosti

Příklady rozsáhlého zpracování:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové tramvajenky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů individuálním právníkem

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b) a c)

4 Co znamená „pravidelné a systematické monitorování“?

Pojem pravidelné a systematické monitorování subjektů údajů Obecné nařízení nedefinuje, jasně však tento výraz zahrnuje všechny formy sledování a profilování na internetu, i pro účely behaviorální reklamy. Pojem monitorování není ovšem omezen pouze na prostředí online.

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů: provozování telekomunikační sítě; poskytování telekomunikačních služeb; cílení internetové reklamy pomocí e-mailového retargetingu, marketing řízený daty, profilování a bodování (skórování) pro účely posouzení rizik (např. pro účely hodnocení úvěrového rizika, stanovení výše pojistného, předcházení podvodům, odhalování praní špinavých peněz), sledování polohy, například u mobilních aplikací; věrnostní programy; behaviorální reklama; sledování zdravého životního stylu, tělesné kondice a zdravotních dat pomocí na těle nositelných zařízení, kamerové systémy, propojená zařízení, např. chytré měřiče, chytrá auta, inteligentní domy (domotika), atd.

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanovených časech
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b)

5 Mohou organizace jmenovat pověřence společně? Pokud ano, za jakých podmínek?

Ano. Skupina podniků může jmenovat jediného pověřence, pokud bude „snadno dosažitelný z každého podniku“. Pojem dosažitelnost se vztahuje k úkolům pověřence coby kontaktního místa pro subjekty údajů, dozorové úřady a platí také interně, uvnitř organizace. Pro zabezpečení dosažitelnosti pověřence, interního nebo externího, je důležité zajistit dostupnost jeho kontaktních údajů. Pověřenec, pokud nutno s pomocí týmu, musí být schopen účinně

komunikovat se subjekty údajů a spolupracovat s dotčenými dozorovými orgány. To znamená, že komunikace musí probíhat v jazyce nebo jazycích užívaných dotčenými dozorovými orgány a subjekty údajů. Dosažitelnost pověřence (fyzicky na stejném pracovišti jako zaměstnanci, přes horkou linku nebo bezpečné komunikační prostředky) je zásadní pro zajištění, že subjekty údajů budou schopny pověřence kontaktovat.

Jediný pověřenec může být jmenován pro několik orgánů veřejné moci nebo veřejných subjektů s přihlédnutím k jejich organizační struktuře a velikosti. Pro zdroje a komunikaci platí stejná kritéria. Vzhledem k tomu, že pověřenec má rozmanité úkoly, musí správce nebo zpracovatel zajistit, aby je jediný pověřenec, pokud nutno s pomocí týmu, mohl vykonávat efektivně i navzdory skutečnosti, že byl jmenován pro několik orgánů veřejné moci nebo veřejných subjektů.

Zdroj: Obecné nařízení, článek 37, odst. 2 a 3

6 Kde má pověřenec sídlit?

WP29 doporučuje, jako obecné pravidlo, aby pověřenec v zájmu dosažitelnosti sídlil v Evropské unii, bez ohledu, zda správce nebo zpracovatel je v Evropské unii usazen. Nelze však vyloučit, že v některých situacích, kdy správce nebo zpracovatel nebude mít provozovnu v Evropské unii, může pověřenec vyvíjet činnost účinněji, pokud bude sídlit mimo EU.

7 Lze jmenovat externího pověřence?

Ano. Pověřencem může být pracovník správce nebo zpracovatele (interní pověřenec) nebo může úkoly plnit na základě smlouvy o poskytování služeb. To znamená, že pověřencem může být externista a v takovém případě vykonává svoji funkci na základě smlouvy o poskytování služeb uzavřené s jednotlivcem nebo organizací.

Vykonává-li funkci pověřence externí poskytovatel, pak úkoly pověřence mohou být plněny týmově jednotlivci pracujícími pro daného externistu, přičemž odpovědnost nese určená vedoucí kontaktní osoba pověřená péčí o klienta. V tomto případě je nezbytné, aby každý člen externí organizace vykonávající funkci pověřence plnil všechny příslušné požadavky Obecného nařízení.

V zájmu právní jasnosti a dobré organizace a také kvůli prevenci konfliktu zájmů se doporučuje mít ve smlouvě o poskytování služeb jasné rozdělení úkolů v rámci týmu externího pověřence a ustanovit jednu určitou osobu jako hlavní kontakt pověřený péčí o klienta.

Zdroj: Obecné nařízení, článek 37, odst. 6

8 Jaké profesní kvality by pověřenec měl mít?

Pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly.

Potřebná úroveň odborných znalostí by měla být určena v závislosti na prováděných zpracovatelských operacích a požadované ochraně zpracovávaných osobních údajů. Pokud například je zpracovatelská činnost zvláště složitá nebo je prováděna s velkým množstvím citlivých údajů, bude pověřenec potřebovat znalosti a podporu na vyšší úrovni.

Mezi důležité dovednosti a zkušenosti patří:

- znalost národního a unijního práva v oblasti ochrany dat a praktické zkušenosti včetně hluboké znalosti Obecného nařízení
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat

- znalost dané oblasti podnikání a organizace
- schopnost propagovat kulturu ochrany dat v organizaci

Zdroj: Obecné nařízení, článek 37, odst. 5

Postavení pověřence

9 Jaké zdroje by správce nebo zpracovatel měl pověřenci poskytnout pro plnění úkolů?

Pověřenec musí mít zdroje potřebné k výkonu svých úkolů.

V závislosti na povaze zpracovatelských operací a činností a velikosti organizace jsou zdroje, které by pověřenec měl mít k dispozici, následující:

- aktivní podpora ze strany vyššího managementu
- dostatek času k plnění úkolů
- odpovídající podpora finanční, technická (kancelářské prostory, vybavení, zařízení) a personální pokud je potřeba
- oficiální oznámení o jmenování pověřence všem zaměstnancům
- přístup do jiných útvarů v organizaci, aby měl pověřenec nezbytnou podporu a informace z těchto útvarů
- průběžné školení

Zdroj: Obecné nařízení, článek 38, odst. 2

10 Jaké jsou záruky umožňující pověřenci plnit úkoly nezávislým způsobem? Co znamená „konflikt zájmů“?

Existuje několik záruk umožňujících pověřenci konat nezávisle:

- žádné pokyny od správce nebo zpracovatele týkající se výkonu úkolů pověřence
- nemožnost propuštění nebo sankcionování v souvislosti s plněním úkolů
- zajištění správcem nebo zpracovatelem, aby žádné pověřencovy úkoly nebo povinnosti nevedly ke střetu zájmů

Jiné úkoly pověřence nesmějí vést ke konfliktu zájmů. V první řadě to znamená, že pověřenec nemůže v organizaci zastávat místo, na kterém by musel stanovovat účely a prostředky zpracování osobních údajů. Vzhledem k organizační struktuře specifické pro každou organizaci, je potřeba tuto otázku řešit případ od případu.

V konfliktním postavení uvnitř organizace mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování. Konflikt zájmů může také kupříkladu vzniknout, pokud externí pověřenec bude požádán o zastupování správce nebo zpracovatele před soudem v případě týkajícím se ochrany osobních údajů.

Zdroj: Obecné nařízení, článek 38, odst. 3 a článek 38, odst. 6

Úkoly pověřence

11 Co znamená „monitorování souladu“?

Pověřenec, v rámci svých povinností, může zejména:

- shromažďovat informace za účelem zjišťování zpracovatelských činností
- analyzovat a prověřovat právní soulad zpracovatelských činností
- informovat, radit a vydávat doporučení správci nebo zpracovateli

Zdroje: Obecné nařízení, článek 39, odst. 1, písm. b)

12 Je pověřenec osobně odpovědný v případě nesouladu s požadavky ohledně ochrany osobních údajů?

Ne. Pověřenci nejsou osobně odpovědní za nesoulad s požadavky ochrany osobních údajů. Je to správce nebo zpracovatel, kdo musí zajistit a doložit, že zpracování probíhá ve shodě s Obecným nařízením. Dodržování předpisů pro ochranu osobních údajů je odpovědností správce nebo zpracovatele.

13 Jaká je role pověřence v souvislosti s posudky vlivu na ochranu osobních údajů a se záznamy o činnostech zpracování?

Pokud jde o posouzení vlivu na ochranu osobních údajů, správce nebo zpracovatel by si měl nechat pověřencem poradit, mimo jiné v následujících věcech:

- zda je potřeba, případně není potřeba, vypracovat posouzení vlivu na ochranu osobních údajů (dále jen „posouzení vlivu“)
- jakou metodiku při zpracování posouzení vlivu uplatnit
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s požadavky na ochranu osobních údajů

V případě záznamů o činnostech zpracování má povinnost vést záznamy o zpracovatelských operacích správce nebo zpracovatel, nikoliv pověřenec. Nic ovšem nebrání správci nebo zpracovateli, aby pověřenci zadal úkol vést záznamy o operacích zpracování, přičemž odpovědnost nese správce nebo zpracovatel. Tyto záznamy by měly být chápány jako jeden z nástrojů umožňující pověřenci vykonávat úkoly spočívající v monitorování souladu, informování a poskytování rad správci nebo zpracovateli.

Zdroj: Obecné nařízení, článek 39, odst. 1, písm. c) a článek 30

V Bruselu dne 13. prosince 2016

*Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN*

Posledně revidováno a schváleno 5. dubna 2017

*Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN*