24. 1. 2017

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Pověřenec pro ochranu osobních údajů dle nařízení GDPR – Nové pokyny WP29 k výkonu funkce

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů známé pod zkratkou GDPR k datu své účinnosti (25. května 2018) zásadně promění právní úpravu ochrany osobních údajů v členských státech EU. Jednou z významných novinek, kterou přináší do českého právního řádu, je role tzv. pověřence pro ochranu osobních údajů. Tento článek se zabývá některými otázkami spojenými s touto rolí, a to v kontextu nedávno zveřejněného výkladového stanoviska pracovní skupiny WP29.

Becker & Poliakoff
advokátní kancelář

Nařízení GDPR[1] nově na celoevropské úrovni zavádí funkci „pověřence pro ochranu osobních údajů“, někdy označovaného také jako inspektor ochrany osobních údajů, angl. *Data Protection Officer – DPO* (dále jen „**pověřenec**“).[2] Přestože obdobný institut je již v některých členských státech znám, pro české prostředí je tato role zcela nová. Pověřenec pro ochranu osobních údajů má podle nařízení GDPR plnit funkci pomocníka či koordinátora ochrany osobních údajů příslušného správce nebo zpracovatele a zároveň funkci jakéhosi kontaktního bodu pro jeho komunikaci s dozorovými úřady (v ČR s Úřadem pro ochranu osobních údajů).

Pracovní skupina pro ochranu osobních údajů (angl. *The Article 29 Data Protection Working Party*; dále jen „**pracovní skupina WP29**“)[3] vydala 13. prosince minulého roku první výkladová stanoviska[4] k některým významným otázkám nařízení GDPR; jedno z nich se podrobněji zabývá právě pověřencem pro ochranu osobních údajů. Z naší praxe je nám známo, že správné uchopení tohoto institutu u některých adresátů normy přináší řadu pochopitelných otázek týkajících se např. povinnosti funkci ustavit, postavení pověřence, jeho úkolů atd. Cílem tohoto článku je proto přiblížit čtenáři zmíněné výkladové stanovisko pracovní skupiny WP29 s názvem „Pokyny k pověřenci pro ochranu osobních údajů“ (angl. *Guidelines on Data Protection Officers (´DPOs´)*; dále jen „**Pokyny**“).

Jmenování pověřence pro ochranu osobních údajů

Povinné jmenování pověřence pro ochranu osobních údajů předepisuje nařízení GDPR v článku 37 pro následující případy:

- zpracování osobních údajů provádí orgán veřejné moci nebo veřejný subjekt (nehledě na to, jaké kategorie osobních údajů a v jaké míře zpracovává);
- hlavní činnosti správce nebo zpracovatele spočívají ve zpracování údajů, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů[5] nebo údajů týkajících se rozsudků v trestních věcech a trestných činů; nebo

- vyžaduje-li tak právo Evropské unie nebo členského státu.

Jak je patrné, Nařízení operuje s poměrně vágními pojmy jako *„hlavní činnost“*, *„rozsáhlý“* nebo *„pravidelný a systematický“* a nechává tak prostor pro více možných výkladů. Pro odstranění výkladových pochybností pracovní skupina WP29 podává v Pokynech bližší výklad těchto pojmových znaků, jejichž naplnění zakládá povinnost správce nebo zpracovatele osobních údajů jmenovat pověřence, a zároveň uvádí některé případy, které je podle jejího názoru možné pod tyto pojmy podřadit.

K výkladu některých pojmů

Za „hlavní činnosti“ (angl. *core activities*) správce nebo zpracovatele mají být podle Nařízení považovány ty činnosti, které souvisejí s jeho základními obchodními a provozními činnostmi (předmětem podnikání). Jmenování pověřence by tak nemělo být pro správce povinné v případě zpracování osobních údajů, které je prováděno pouze jako pomocná činnost k dosažení základních cílů činnosti správce. Pracovní skupina WP29 výslovně uvádí, že společnosti běžně provádějí různé podpůrné činnosti (jako například vedení evidence za účelem vyplácení mezd zaměstnancům), které jsou nezbytné k zajištění hlavní činnosti společnosti. Tyto činnosti však nelze ve většině případů považovat za hlavní činnost správce. Na druhou stranu v případech, kdy zpracování osobních údajů je neodmyslitelnou součástí činnosti správce nebo zpracovatele, mělo by být považováno za hlavní činnost – jako příklad uvádí pracovní skupina WP29 zpracování zdravotních údajů pacientů jako jednu z hlavních činností nemocnice.

Nařízení zavádí povinnost jmenovat pověřence pro ochranu osobních údajů mimo jiné v situacích, kdy hlavní činnosti správce nebo zpracovatele spočívají ve zpracování vyžadujícím *„rozsáhlé“* pravidelné a systematické monitorování nebo v *„rozsáhlém“* zpracování tzv. zvláštních kategorií údajů. Nařízení samo nespecifikuje pojem *„rozsáhlý“* (angl. *large scale*), což u řady správců a zpracovatelů osobních údajů může vyvolat právní nejistotu ohledně toho, zda mají funkci pověřence zřizovat a obsazovat, či nikoliv. Pracovní skupina WP29 doporučuje pro určení toho, zdali je prováděno rozsáhlé zpracování osobních údajů, zvážit zejména množství zpracovávaných osobních údajů (jak množství zpracovávaných údajů obecně, tak v poměru k relevantní populaci), různorodost zpracovávaných osobních údajů, dobu trvání zpracovávání osobních údajů či geografický rozsah území, ze kterého pochází zpracovávané osobní údaje.

Jako příklad rozsáhlého zpracování uvádí pracovní skupina WP29 mimo jiné zpracování osobních údajů pacientů nemocnicí (nikoliv však zpracování osobních údajů jednotlivým lékařem), zpracování osobních údajů zákazníků pojišťovnou nebo bankou či zpracování osobních údajů za účelem personalizování obsahu a cílení reklamy na základě chování při používání vyhledávacích nástrojů (angl. *behavioural advertising by a search engine*).

K pojmu *„pravidelné a systematické monitorování“* (angl. *regular and systematic monitoring*) pracovní skupina W29 poznamenává, že samotný pojem „monitorování“ se nevztahuje výlučně na online prostředí,[6] ale i na jiné monitorování subjektu údajů. Pojem *„pravidelný“* má podle pracovní skupiny WP29 jeden z následujících významů: i) probíhající nebo v určitých (rozsáhlejších) intervalech po určitou (delší) dobu trvající; ii) opakované nebo opakující se ve stanovených časech; nebo iii) nepřetržité nebo periodicky se opakující.

Pojem *„systematický“* má být vykládán jako: i) vyskytující se podle určité systematiky; ii) předem uspořádaný, organizovaný nebo metodický; iii) vyskytující se jako část obecného plánu sběru dat; nebo iv) prováděný jako součást strategie. Jako praktické příklady „pravidelného a systematického monitorování“ uvádí pracovní skupina WP29 zejména provozování telekomunikačních sítí,

poskytování telekomunikačních služeb, ale i tzv. email retargeting, věrnostní programy (angl. *loyalty programs*) anebo reklamní sdělení cílená na základě chování subjektu údajů při používání vyhledávacích nástrojů (angl. *behavioural advertising*).

Co dělat v případě, že není dána povinnost jmenovat pověřence?

Z výše uvedeného vyplývá, že povinnost ustavit funkci pověřence pro ochranu osobních údajů, jmenovat jej a vybavit příslušnými kompetencemi není dána vždy. V každém případě bude záležet na posouzení, zda spadá zpracování osobních údajů subjektů mezi hlavní činnosti správce anebo zpracovatele.

Pracovní skupina WP29 však doporučuje, aby každý správce anebo zpracovatel, který pověřence nejmenuje, disponoval stanoviskem, či odůvodněním, proč nepovažuje podmínky nařízení GDPR pro povinné jmenování pověřence v rámci své obchodní a provozní činnosti za naplněné. Jinak řečeno, je doporučenou praxí provést vnitřní analýzu a připravit dokument obecné povahy, v němž bude doloženo, že (a proč) není hlavní činností správce nebo zpracovatele rozsáhlé pravidelné a systematické monitorování subjektů údajů anebo zpracování zvláštních kategorií osobních údajů.

V případě, že se správce nebo zpracovatel, který není k jmenování pověřence povinen, rozhodne jmenovat pověřence dobrovolně, uplatní se na jeho jmenování, postavení a úkoly stejné zákonné požadavky, jakoby se jednalo o povinně jmenovaného pověřence. Správci nebo zpracovateli rovněž nic nebrání v tom, aby otázkami ochrany osobních údajů pověřil svého zaměstnance nebo externího poradce jakožto „konzultanta," který však nesmí jednat a navenek působit jako pověřenec.

Článek 37 odst. 2 nařízení GDPR umožňuje skupině podniků jmenovat jediného pověřence pro ochranu osobních údajů, pokud je snadno dosažitelný z každého podniku. Pracovní skupina W29 pak v Pokynech blíže konkretizuje pojem „snadné dosažitelnosti", a to tak, že pověřenec musí být schopen účinně komunikovat jak se subjekty údajů, tak s každým z podniků a zároveň spolupracovat s dozorovými úřady. Proto, aby se mohly subjekty údajů snadno obracet na pověřence, je dle Pokynů zásadní jeho osobní fyzická dostupnost, což zahrnuje také možnost obrátit se na něj telefonní cestou nebo jinými způsoby přímé komunikace.

Postavení pověřence pro ochranu osobních údajů

Pozici pověřence pro ochranu osobních údajů může správce nebo zpracovatel obsadit jak svým pracovníkem (zaměstnancem), tak externě spolupracující osobou nebo organizací, která bude své úkoly plnit na základě smlouvy o poskytování služeb. Nařízení nestanovuje konkrétní kvalifikační požadavky na pověřence, pouze ve svém článku 37 odst. 5 v obecnosti konstatuje, že pověřenec by měl 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 stanovené Nařízením. Pokyny k tomu upřesňují, že úroveň odbornosti pověřence by měla být zvážena především v souvislosti s citlivostí, provázaností a objemem zpracovávaných osobních údajů. Dále by měl mít pověřenec znalosti v oblasti národní i evropské oblasti ochrany osobních údajů a hluboké znalosti Nařízení. Užitečnou znalostí je zajisté orientace v oblasti businessu a ve vnitřním uspořádání správce.

Pověřenec pro ochranu osobních údajů má být podle článku 38 odst. 1 nařízení GDPR *náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů*. Pracovní skupina WP29 doporučuje, aby správce nebo zpracovatel zajistil odpovídající míru kompetence a pravomocí na straně pověřence, například tím, že pověřence přizve k pravidelným schůzkám vyššího a středního managementu, zajistí účast a stanovisko pověřence v situacích, kdy jsou přijímána rozhodnutí, která se mohou dotknout ochrany osobních údajů, poskytne pověřenci všechny relevantní informace v

dostatečné lhůtě, aby k nim mohl vyjádřit své stanovisko, zajistí, aby názoru pověřence na situaci, která se dotýká oblasti ochrany osobních údajů, byla vždy přikládána váha (pokud s názorem pověřence vedení společnosti nesouhlasí, doporučuje pracovní skupina WP29 zdokumentovat důvody, které vedly k nevyslyšení stanoviska pověřence), zajistí okamžité informování pověřence po porušení zabezpečení osobních údajů nebo jiném bezpečnostním incidentu atp.

Nařízení dále v článku 38 odst. 2 ukládá správci či zpracovateli povinnost podporovat pověřence pro ochranu osobních údajů při plnění jeho úkolů tím, že mu poskytne *zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí*. Za tyto zdroje Pracovní skupina WP29 považuje zejména:

- oficiální jmenování pověřence a oznámení tohoto jmenování všem zaměstnancům a pracovníkům podniku;
- nezbytný přístup a komunikaci s jinými podnikovými odděleními (HR, právní, bezpečnostní, IT oddělení aj.);
- poskytnutí dostatečného času, vybavení a případně personálního zázemí, aby mohl pověřenec vykonávat své povinnosti;
- odpovídající finanční ohodnocení;
- aktivní podporu pověřence ze strany vyššího managementu v ostatních otázkách souvisejících s ochranou osobních údajů (např. možnost vzdělávání v oblasti ochrany osobních údajů).

Pro řádné plnění úkolů pověřence pro ochranu osobních údajů požaduje Nařízení nezávislé postavení pověřence na správci nebo zpracovateli, které se projevuje mimo jiné tím, že mu nesmějí být udělovány žádné pokyny týkající se výkonu těchto úkolů, v souvislosti s plněním svých úkolů nesmí být správcem nebo zpracovatelem propuštěn ani sankcionován a v rámci organizační hierarchie společnosti má být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.

Pracovní skupina WP29 dále doporučuje pro případy velkého množství zpracovávaných osobních údajů sestavení zvláštního „DPO týmu“ (popř. samostatné organizační jednotky, sekce, oddělení) pro ochranu osobních údajů s pověřencem v čele.

Úkoly pověřence pro ochranu osobních údajů

Nařízení předepisuje pověřenci několik úkolů a povinností. Mezi ty hlavní řadí sledování souladu vnitřní praxe podniku s právní úpravou ochrany osobních údajů. Podle pracovní skupiny WP29 je zejména vhodné, aby pověřenec sbíral informace k preciznímu rozpoznání a vymezení zpracovávání osobních údajů, analyzoval a kontroloval shodu vnitřní praxe zpracovávání s právní úpravou, či informoval, radil a vydával doporučení pro správce nebo zpracovatele osobních údajů.

Mezi další úkoly pověřence řadí nařízení GDPR v článku 35 odst. 1 poradní funkci v průběhu nově upraveného procesu, kterým je provádění posouzení vlivu na ochranu osobních údajů (angl. *Data Protection Impact Assessment – DPIA*). K tomuto Pracovní skupina WP29 doporučuje v první řadě provést analýzu, zda je posouzení vlivu na ochranu osobních údajů v daném případě nezbytné, vybrat vhodnou metodu pro provedení posouzení vlivu na ochranu osobních údajů a posoudit, jaké záruky (včetně technických a organizačních opatření) se mají aplikovat k tomu, aby se snížilo riziko pro práva a zájmy subjektů údajů.

Nařízení GDPR povoluje správci pověřit pověřence i jinými úkoly a povinnostmi. Dle Pokynů je však správce povinen zajistit, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů na straně pověřence; neexistence konfliktu zájmů je úzce spojena s požadavkem na jeho nezávislé chování. Přestože je pověřencům umožněno vykonávat i jiné funkce a úkoly, ty jim však mohou být svěřeny

pouze tehdy, pokud nejsou v pozici konfliktu zájmů s výkonem funkce pověřence (např. pověřenec nemůže zároveň působit na pozici, ve které by určoval účely a důvody zpracovávání osobních údajů).

Za dobrou praxi považuje pracovní skupina WP29 obecně interní označení pozic nekompatibilních s pozicí pověřence; nastavení vnitřních postupů v případě konfliktu zájmů v osobě vykonávající funkci pověřence; formulaci obecného vysvětlení, co to je v tomto případě konflikt zájmů a prohlásit, že konkrétní pověřenec není v konfliktu zájmů; zahrnutí „záchranných ustanovení“ do vnitřních pravidel společnosti, které zajistí, že nabízená pozice pověřence pro ochranu osobních údajů nebo smlouva o poskytování služeb je dostatečně přesná a konkrétní, aby vyloučila možný konflikt zájmů v osobě budoucího pověřence.

Místo závěru

Správci a zpracovatelé osobních údajů by měli i s ohledem na výkladová stanoviska pracovní skupiny WP29 obsažená v Pokynech důkladně zvážit, zda se na ně vztahuje povinné jmenování pověřence pro ochranu osobních údajů, a v opačném případě rozhodnout, zda není vhodné zřídit tuto funkci dobrovolně. Jmenováním pověřence se sice, jak zdůrazňují Pokyny, správce či zpracovatele osobních údajů nezbavuje odpovědnosti za zajištění ochrany osobních údajů v souladu s Nařízením, jeho jmenování si však může usnadnit zajištění plnění povinností v oblasti ochrany osobních údajů a v případě porušení Nařízení zmírnit svou odpovědnost poukazem na to, že vynaložil veškeré úsilí k dodržení „best practice“ v oblasti ochrany osobních údajů.

V každém případě lze správcům a zpracovatelům doporučit, aby bedlivě sledovali vývoj v oblasti ochrany osobních údajů i z pohledu povinnosti jmenovat pověřence pro ochranu osobních údajů, a to jak z hlediska prováděcích národních předpisů, tak z pohledu výkladu Nařízení, které se může s ohledem na praxi v průběhu času měnit.

JUDr. Ing. Jindřich Kalíšek,
advokát

Mgr. Ing. Petra Věžníková,
advokátní koncipientka

Becker & Poliakoff, s.r.o., advokátní kancelář

U Prašné brány 1078/1
110 00 Praha 1

Tel: +420 224 900 000
Fax: +420 224 900 041
e-mail: office@becker-poliakoff.cz

_____
[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 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/EU, dostupné na www, k dispozici >>> zde (dále jen jako „nařízení GDPR“ anebo „Nařízení“).
[2] Oficiální český překlad nařízení GDPR důsledně užívá termín „pověřenec pro ochranu osobních údajů“; toho se budeme držet i v tomto článku.
[3] Pracovní skupina ustanovená čl. 29 Směrnice Evropského parlamentu a Rady 95/46/EC ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů funguje v současné době jako nezávislý evropský poradní orgán v oblasti ochrany dat a soukromí. Nejpozději ke dni účinnosti nařízení GDPR však převezme funkce tohoto poradního orgánu Evropský sbor pro ochranu osobních údajů (angl. European Data Protection Board – EDPB) zřízený článkem 68 předmětného nařízení za účelem podpory jeho důsledného uplatňování.
[4] Pracovní skupina WP29 přijala 13. prosince 2016 celkem tři výkladová stanoviska: Pokyny k právu na přenositelnost údajů („Guidelines on the right to data portability“, 16/EN, WP 242), Pokyny k pověřenci pro ochranu osobních údajů („Guidelines on Data Protection Officers (´DPOs´)“, 16/EN, WP 243) a Pokyny k určení vedoucího dozorového úřadu („Guidelines for identifying a controller or processor´s lead supervisory authority“, 16/EN, WP 244).
[5] Tzv. zvláštní kategorií osobních údajů se podle článku 9 odst. 1 nařízení GDPR rozumí osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a dále genetické údaje, biometrické údaje (zpracovávané za účelem jedinečné identifikace fyzické osoby) a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
[6] Výklad obdobného pojmu „monitorování chování subjektu údajů“, který je uveden v bodě 24 Preambule nařízení GDPR, se vztahuje k sledování fyzických osob na internetu a týká se zpracování osobních údajů správcem usazeným mimo EU.

Další články:

- DEAL MONITOR
- Tři dekády v advokacii a otevřený pohled na to, co profesi i justici nejvíc škodí
- DEAL MONITOR
- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR