

WP243 PŘÍLOHA – ČASTO Kladené otázky

Cílem této přílohy je zodpovědět zjednodušenou a snadno čitelnou formou některé klíčové otázky, které mohou organizace mít, pokud jde o nové požadavky obecného nařízení o ochraně osobních údajů týkající se jmenování pověřence pro ochranu osobních údajů.

Jmenování pověřence pro ochranu osobních údajů (článek 37)

1 Které organizace musejí jmenovat pověřence pro ochranu osobních údajů? (čl. 37 odst. 1)

Obecné nařízení o ochraně osobních údajů vyžaduje jmenování pověřence pro ochranu osobních údajů ve třech konkrétních případech:

- je-li zpracování prováděno orgánem veřejné moci nebo veřejným subjektem (bez ohledu na to, jaké údaje jsou zpracovávány),
- spočívají-li hlavní činnosti správce nebo zpracovatele v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; a
- spočívají-li hlavní činnosti správce nebo zpracovatele v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Je třeba poznamenat, že právo Unie nebo členského státu může vyžadovat jmenování pověřenců pro ochranu osobních údajů také v jiných situacích. A konečně, i když obecné nařízení o ochraně osobních údajů jmenování pověřence pro ochranu osobních údajů konkrétně nevyžaduje, pro organizace může být někdy užitečné jmenovat pověřence pro ochranu osobních údajů dobrovolně. Pracovní skupina pro ochranu údajů zřízená podle článku 29 (dále jen „pracovní skupina WP29“) toto dobrovolné úsilí podporuje.

Více informací viz oddíl 2.1 pokynů.

2 Co znamená pojem „hlavní činnosti“? (čl. 37 odst. 1 písm. b) a c))

„Hlavní činnosti“ mohou být považovány za klíčové operace pro dosažení cílů správce nebo zpracovatele. Zahrnují rovněž veškeré činnosti, kde zpracování údajů tvoří neoddělitelnou část činnosti správce nebo zpracovatele. Například zpracování údajů o zdravotním stavu, jako například zdravotních záznamů pacientů, by mělo být považováno za jednu z hlavních činností jakékoli nemocnice, a nemocnice proto musejí jmenovat pověřence pro ochranu osobních údajů.

Na druhou stranu veškeré organizace vykonávají určité podpůrné činnosti, například vyplácení svých zaměstnanců nebo standardní činnosti v oblasti podpory informačních technologií. Toto jsou nezbytné podpůrné funkce pro hlavní činnost organizace nebo hlavní podnikatelskou činnost. Přestože jsou tyto činnosti nezbytné nebo zásadní, obvykle jsou považovány za pomocné funkce spíše než za hlavní činnost.

Více informací viz oddíl 2.1.2 pokynů.

3 Co znamená pojem „rozsáhlý“ ? (čl. 37 odst. 1 písm. b) a c))

Obecné nařízení o ochraně osobních údajů nedefinuje, co znamená rozsáhlé zpracování. Pracovní skupina W29 doporučuje, aby byly při určování toho, zda je zpracování prováděno ve velkém rozsahu, vzaty v úvahu především tyto faktory:

- počet dotčených subjektů údajů – buď jako konkrétní číslo, nebo jako podíl příslušné skupiny obyvatelstva,
- objem údajů a/nebo škálu různých údajových položek, které jsou zpracovávány,
- trvání nebo stálost činnosti zpracování údajů,
- zeměpisný rozsah činnosti zpracování.

Příklady zpracování ve velkém rozsahu zahrnují:

- zpracování údajů pacientů v rámci pravidelné činnosti provedené nemocnicí,
- zpracování cestovních údajů jednotlivců používajících systém městské hromadné dopravy (např. sledování prostřednictvím cestovních karet),
- zpracování údajů o zeměpisné poloze v reálném čase zákazníků mezinárodního řetězce rychlého občerstvení pro statické účely, a to zpracovatelem specializujícím se na poskytování těchto činností,
- zpracování údajů zákazníků v rámci pravidelné činnosti provedené pojišťovnou nebo bankou,
- zpracování osobních údajů pro behaviorální reklamu provedené vyhledávačem,
- zpracování údajů (obsah, provoz, umístění) provedené poskytovatelem telefonních nebo internetových služeb.

Příklady, které nepředstavují zpracování ve velkém rozsahu, zahrnují:

- zpracování údajů pacientů provedené jednotlivým lékařem,
- zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů provedené jednotlivým právníkem.

Více informací viz oddíl 2.1.3 pokynů.

4 Co znamená pojem „pravidelné a systematické monitorování“? (čl. 37 odst. 1 písm. b))

Obecné nařízení o ochraně osobních údajů pojem pravidelného a systematického monitorování subjektů údajů nedefinuje, jasně však zahrnuje veškeré formy sledování a profilování na internetu, a to i pro účely behaviorální reklamy. Pojem monitorování však není omezen na on-line prostředí.

Pracovní skupina WP29 vykládá pojem „pravidelné“ v tom smyslu, že znamená jedno nebo více z níže uvedeného:

- probíhající nebo vyskytující se po určité období v určitých intervalech,
- opakovaně se vyskytující nebo opakované ve stanovených časech,
- odehrávající se nepřetržitě nebo pravidelně.

Pracovní skupina WP29 vykládá pojem „systematické“ v tom smyslu, že znamená jedno nebo více z níže uvedeného:

- vyskytující se v souladu se systémem,
- předem naplánované, organizované nebo metodické,

- odehrávající se jako součást obecného plánu pro shromažďování údajů,
- provedené jako součást strategie.

Příklady: provozování telekomunikačních sítí, poskytování telekomunikačních služeb, přesměrovávání elektronické pošty, profilování a bodování pro účely posouzení rizik (např. pro účely úvěrového ohodnocení, stanovení pojistného, předcházení podvodům, zjištění praní špinavých peněz), sledování polohy, například prostřednictvím mobilních aplikací, věrnostní programy, behaviorální reklama, monitorování údajů o psychické a fyzické zdatnosti a zdravotním stavu prostřednictvím zařízení nošených na těle, uzavřené televizní okruhy, propojená zařízení, např. inteligentní měřiče, inteligentní automobily, automatizace v oblasti bydlení atd.

Více informací viz oddíl 2.1.4 pokynů.

5 Mohou organizace jmenovat pověřence pro ochranu osobních údajů společně? Pokud ano, za jakých podmínek? (čl. 37 odst. 2 a 3)

Obecné nařízení o ochraně osobních údajů stanoví, že skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů, pokud je „*snadno dosažitelný z každého podniku*“. Pojem dosažitelnosti odkazuje na úkoly pověřence pro ochranu osobních údajů jakožto kontaktní místo, pokud jde o subjekty údajů, dozorový úřad, ale také interně uvnitř organizace. Aby se zajistilo, že pověřenec pro ochranu osobních údajů, ať už interní nebo externí, je dosažitelný, je důležité zajistit dostupnost jeho kontaktních údajů v souladu s obecným nařízením pro ochranu osobních údajů. Pověřenec musí být schopen účinně komunikovat se subjekty údajů a spolupracovat s dotčenými dozorovými úřady. To znamená, že tato komunikace musí probíhat v jazyce nebo jazycích používaných dozorovými úřady a dotčenými subjekty údajů. Osobní dosažitelnost pověřence pro ochranu osobních údajů (ať už fyzicky ve stejných prostorách jako zaměstnanci, prostřednictvím horké linky nebo jiných bezpečných komunikačních prostředků) je zásadní pro zajištění toho, aby se subjekty údajů mohly na pověřence pro ochranu osobních údajů obrátit.

Více informací viz oddíl 2.3 pokynů.

6 Je možné jmenovat externího pověřence pro ochranu osobních údajů (čl. 37 odst. 6)?

Ano. Podle čl. 37 odst. 6 může být pověřenec pro ochranu osobních údajů pracovníkem správce či zpracovatele (interní pověřenec pro ochranu osobních údajů), nebo může „*úkoly plnit na základě smlouvy o poskytování služeb*“. To znamená, že pověřenec pro ochranu osobních údajů může být externí, a v tomto případě může být jeho funkce vykonávána na základě smlouvy o poskytování služeb uzavřené s jednotlivcem nebo s organizací.

Je-li pověřenec pro ochranu osobních údajů externí, vztahují se na něj veškeré požadavky podle článků 37 až 39. Jak je uvedeno v pokynech, je-li funkce pověřence pro ochranu osobních údajů vykonávána externím poskytovatelem služeb, skupina osob pracujících pro tento subjekt může účinně plnit úkoly pověřence pro ochranu osobních údajů jako tým, za který je odpovědný určený hlavní kontakt a „*odpovědná osoba*“ pro klienta. V tomto případě je nezbytné, aby každý člen externí organizace vykonávající funkce pověřence pro ochranu osobních údajů splňoval veškeré příslušné požadavky obecného nařízení o ochraně osobních údajů.

V zájmu právní jasnosti a dobré organizace pokyny doporučují ve smlouvě o poskytování služeb jasně rozdělit úkoly v rámci externího týmu pověřenců pro ochranu osobních údajů a určit jednu osobu jakožto hlavní kontakt a „odpovědnou“ osobu pro klienta.

Více informací viz oddíly 2.3, 2.4 a 3.5 pokynů.

7 Jaké by měl mít pověřenec pro ochranu osobních údajů profesní kvality (čl. 37 odst. 5)?

Obecné nařízení o ochraně osobních údajů stanoví, že pověřenec pro ochranu osobních údajů „*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 stanovené v článku 39*“.

Potřebná úroveň odborných znalostí by se měla určit podle prováděných operací zpracování údajů a podle ochrany, která se vyžaduje pro zpracovávané osobní údaje. Například je-li činnost zpracování údajů zvláště složitá nebo zahrnuje-li velké množství citlivých údajů, může pověřenec pro ochranu osobních údajů potřebovat vyšší úroveň odborných znalostí a podpory.

Nezbytné dovednosti a odborné znalosti zahrnují:

- odborné znalosti v oblasti vnitrostátní a evropské praxe a právních předpisů na ochranu údajů, včetně důkladného chápání obecného nařízení o ochraně osobních údajů,
- porozumění prováděným operacím zpracování
- porozumění informačním technologiím a zabezpečení osobních údajů,
- znalost podnikatelského odvětví a organizace,
- schopnost prosazovat v rámci organizace kulturu ochrany osobních údajů.

Více informací viz oddíl 2.4 pokynů.

Postavení pověřence pro ochranu osobních údajů (článek 38)

8 Jaké zdroje by měly být poskytnuty pověřenci pro ochranu osobních údajů k provádění jeho úkolů?

Čl. 38 odst. 2 obecného nařízení o ochraně osobních údajů vyžaduje, aby organizace podporovala své pověřence pro ochranu osobních údajů tím, „*že jim poskytne zdroje nezbytné k plnění [jejich] úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí*“.

V závislosti na povaze operací zpracování a na činnostech a velikosti organizace by pověřenci pro ochranu osobních údajů měly být poskytnuty tyto zdroje:

- aktivní podpora funkce pověřence pro ochranu osobních údajů ze strany vedoucích pracovníků,
- dostatečný čas na to, aby mohli pověřenci pro ochranu osobních údajů plnit své povinnosti,
- odpovídající podpora z hlediska finančních zdrojů, infrastruktury (prostory, zařízení, vybavení) a případně pracovníků,
- oficiální oznámení všem zaměstnancům o jmenování pověřence pro ochranu osobních údajů,
- přístup k dalším službám v rámci organizace, aby se zajistilo, že pověřenci pro ochranu osobních údajů mohou od těchto dalších služeb obdržet základní podporu, vstupy nebo informace,
- průběžné školení.

Více informací viz oddíl 3.2 pokynů.

9 Jaké jsou záruky umožňující pověřenci pro ochranu osobních údajů plnit své úkoly nezávislým způsobem (čl. 38 odst. 3)?

Existuje několik záruk, které pověřenci pro ochranu osobních údajů umožňují jednat nezávislým způsobem, jak je uvedeno v 97. bodě odůvodnění:

- nedostává pokyny od správců nebo zpracovatelů týkající se výkonu úkolů pověřence pro ochranu osobních údajů,
- nebude propuštěn nebo sankcionován ze strany správců nebo zpracovatelů v souvislosti s výkonem úkolů pověřence pro ochranu osobních údajů,
- nedochází ke střetu zájmů s dalšími možnými úkoly a povinnostmi.

Více informací viz oddíly 3.3 až 3.5 pokynů.

10 Jaké jsou „další úkoly a povinnosti“ pověřence pro ochranu osobních údajů, které mohou vést ke střetu zájmů (čl. 38 odst. 6)?

Pověřenec pro ochranu osobních údajů nesmí v rámci organizace zastávat pozici, ve které by měl určovat účely a prostředky zpracování osobních údajů. Vzhledem ke specifické organizační struktuře každé organizace je toto třeba posoudit individuálně.

Obecně platí, že pozice, které by mohly vést ke střetu zájmů, mohou zahrnovat pozice vedoucího pracovníka (jako například generální ředitel, vedoucí provozní pracovník, finanční ředitel, ředitel oddělení zdravotnictví, vedoucí marketingového oddělení, vedoucí oddělení lidských zdrojů nebo vedoucí oddělení IT), ale také další úlohy nacházející se v organizační struktuře níže, vedou-li tyto pozice a role k určování účelů a prostředků zpracování.

Více informací viz oddíl 3.5 pokynů.

Úkoly pověřence pro ochranu osobních údajů (článek 39)

11 Co zahrnuje pojem „monitorovat soulad“ s obecným nařízením o ochraně osobních údajů (čl. 39 odst. 1 písm. b))?

Jakožto součást těchto povinností monitorovat soulad mohou pověřenci pro ochranu osobních údajů zejména:

- shromažďovat informace pro určení činností zpracování,
- analyzovat a kontrolovat soulad činností zpracování, a
- informovat správce nebo zpracovatele, poskytovat mu poradenství a vydávat doporučení.

Více informací viz oddíl 4.1 pokynů.

12 Nese pověřenec pro ochranu osobních údajů osobní odpovědnost za nedodržování souladu s obecným nařízením o ochraně osobních údajů?

Ne. Pověřenci pro ochranu osobních údajů nenesou osobní odpovědnost za nedodržování souladu s obecným nařízením o ochraně osobních údajů. Obecné nařízení o ochraně osobních údajů jasně stanoví, že je to správce nebo zpracovatel, kdo musí zajistit a být schopen doložit, že zpracování je prováděno v souladu s nařízením (čl. 24 odst. 1). Dodržování požadavků na ochranu údajů je odpovědností správce nebo zpracovatele.

13 Jaká je úloha pověřence pro ochranu osobních údajů, pokud jde o posouzení vlivu na ochranu osobních údajů (čl. 37 odst. 1 písm. c)) a záznamy o činnostech zpracování (článek 30)?

Pokud jde o posouzení vlivu na ochranu osobních údajů, měl by správce nebo zpracovatel vyhledat posudek pověřence pro ochranu osobních údajů mimo jiné v těchto otázkách:

- zda provádět či neprovádět posouzení vlivu na ochranu osobních údajů,
- jakou metodikou se při provádění posouzení vlivu na ochranu osobních údajů řídit,
- zda provádět posouzení vlivu na ochranu osobních údajů interně v rámci organizace, nebo zda ho nechat vypracovat externě,
- jaké záruky (včetně technických a organizačních opatření) uplatňovat za účelem zmírnění jakýchkoliv rizik pro práva a zájmy subjektů údajů,
- zda posouzení vlivu na ochranu osobních údajů bylo či nebylo provedeno správně a zda jsou jeho závěry (tedy zda přistoupit ke zpracování či nikoliv a jaké záruky uplatnit) v souladu s obecným nařízením o ochraně osobních údajů.

Více informací viz oddíl 4.2 pokynů.

Pokud jde o záznamy o činnostech zpracování, je to správce nebo zpracovatel, nikoliv pověřenec pro ochranu osobních údajů, kdo je povinen vést záznamy o operacích zpracování. Správci nebo zpracovateli však nic nebrání v tom, aby pověřenci pro ochranu osobních údajů uložil úkol vést záznamy o operacích zpracování, za něž správce odpovídá. Tyto záznamy by měly být považovány za jeden z nástrojů umožňujících pověřenci pro ochranu osobních údajů provádět své úkoly monitorování souladu, informování správce nebo zpracovatele a poskytování poradenství pro správce nebo zpracovatele.

Více informací viz oddíl 4.4 pokynů.