Nejčastější pochybení zjištěná při implementaci GDPR

Dne 27. dubna 2016 bylo Evropským parlamentem a Radou EU přijato Nařízení č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, tzv. General Data Protection Regulation (dále jen „GDPR" nebo „Nařízení"), jehož účinnost nastává dnem 25. 5. 2018. GDPR nepředstavuje převratnou novinku na poli ochrany osobních údajů, nicméně přináší řadu nových institutů, kterým je nutno přizpůsobit aktuální stav ochrany osobních údajů ve společnosti.

S ohledem na skutečnost, že novému nařízení GDPR je nutno přizpůsobit celkový stav ochrany osobních údajů ve společnosti, což zahrnuje nejen úpravu, revizi či korekturu interní dokumentace, ale také veškerých procesů ve společnosti, proběhla či v současné chvíli probíhá v mnoha organizacích na území České republiky tzv. GAP analýza. Touto analýzou se rozumí diferenční porovnání souladu současného stavu se stavem požadovaným, tedy porovnání aktuálního stavu a míry ochrany osobních údajů v organizaci, se stavem, jak jej požaduje Nařízení. Tento článek sumarizuje přehledným způsobem nejčastější chyby na poli ochrany osobních údajů, kterých se organizace v dnešní době dopouští a využívá tak rozsáhlých zkušeností autorky získaných při provedených GAP analýzách v jednotlivých organizacích.

Obecně lze porušení rozdělit do 3 základních skupin, a to s ohledem na riziko, které jejich porušení správci osobních údajů hrozí v důsledku kontroly ze strany kontrolního úřadu. Tato tři rizika jsou zejména:

1. **Rozpor s GDPR** – kritický rozpor se základními zásadami GDPR, který může vést až k uložení pokuty v plné výši (tedy 20 000 000 € nebo 4% z celkového ročního obratu společnosti za předchozí finanční rok podle toho, která hodnota je vyšší). Většina těchto porušení pramení z porušení pravidel stanovených v čl. 5 a 6 GDPR a jsou jimi např. – chybějící zákonný titul či jeho jednotlivé náležitosti při zpracování osobních údajů, chybějící účel, zpracování nadbytečného množství údajů apod.
2. **Riziko vzniku bezpečnostního incidentu** – jedná se o zanedbání ochrany či bezpečnosti osobních údajů, resp. jednotlivých opatření tak, že není zajištěno, aby nedocházelo k možnostem náhodného či protiprávního zničení, ztráty, pozměnění, neoprávněného zpřístupnění osobních údajů nebo neoprávněného přístupu k osobním údajům. V tomto případě je pak záhodno uvést, že samotný vznik bezpečnostního incidentu není podmínkou zahájení správního řízení. Pro takové zahájení postačí pouze existence rizika, ohrožení, kdy případný únik nebo ztráta dat je pak pouze přitěžující okolností ovlivňující výši uložené pokuty – obecně je za tato porušení možno uložit pokuty až do výše ½ z maximální výše pokut (tedy 10 000 000 € nebo 2% z celkového ročního obratu společnosti za předchozí finanční rok).
3. **Nesplnění povinností dle GDPR** – zde porušení povinností spočívá zejména v ignoraci či nezakotvení potřebných procesů nebo institutů jasně definovaných GDPR. Jde zvláště o instituty provádění práv subjektů, povinnosti vykonat hloubkovou analýzu posouzení vlivu na ochranu osobních údajů nebo nejmenování pověřence pro ochranu osobních údajů.
   Při vypracování GAP analýzy je vždy nutno mít zcela jasně specifikovaná rizika, která mohou nastat. Tato je pak potřeba vyhodnocovat pro každá jednotlivá zpracování osobních údajů, zda tato rizika hrozí, a to s ohledem na veškerá pravidla a požadavky stanovené GDPR. Tento článek shrnuje některá základní a nejčastější porušení, kterých se organizace dopouští, a co tak může být vyhodnoceno s ohledem na implementaci GDPR jako problematické, či v rozporu. Těmito porušeními jsou:
   - **Není splněna informační povinnost ani na základní úrovni** – tato povinnost, i když v zásadně zjednodušené podobě, je již požadována v současném zák. č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, nicméně její provádění není vždy zcela stoprocentní. GDPR sebou přináší ještě větší prohloubení, resp. zkonkretizování této problematiky, když zásadním způsobem rozšiřuje rozsah informací, které musí správce subjektům poskytovat. V rámci většiny organizací v současné chvíli neprobíhá téměř žádná informační povinnost – subjekty údajů nejsou o zpracování osobních údajů oficiálně informovány, popř. o tomto informování neexistuje záznam.
   - **V rámci organizace jsou zpracovávány údaje, které nejsou nezbytné** – např. v personálních složkách zaměstnanců současných i bývalých (kopie různých dokladů, netřízení složek po odchodu, exekuce apod.)
   - **Fyzické zabezpečení dokumentů je nedostatečné** – ne všechny dokumenty v organizacích jsou chráněny dostatečným a adekvátním způsobem. Většinou spočívá porušení v problematice neřízených přístupů, sdílených, resp. průchozích kanceláří, resp. možnosti přístupu do kanceláře, i když se zde pracovník nenachází, nedostatky v zamykání kanceláří či jednotlivých skříní. Ve většině případů není zavedeno pravidlo čistého stolu. Dalším častým porušením fyzické bezpečnosti je ponechávání dokumentů či soukromých nebo služebních zařízení (např. externích disků, flash disků), bez dozoru, s nedostatečným zabezpečením proti vniknutí, poškození, zcizení či ztrátě. Zároveň se může stát, že v kanceláři či na vrátnici či recepci nebývá přítomna žádná osoba, která by zamezila přístupu neoprávněných osob. Častým problémem bývá neřízené vydávání přístupových klíčů či kódů, existence „univerzálních" klíčů, možnost kopírování klíčů, nezabezpečená okna či nesprávně umístěné kamery (zakrývání, možnost odsunutí) atd.
   - **Digitální zabezpečení dokumentů je nedostatečné** – zásadní problémy digitální ochrany jsou spatřovány spíše celkově – nedostatky se promítají v celém systému IT jednotlivých společností. V rámci informačních technologií lze za největší nedostatek považovat absenci přijatých technických opatření, jakými jsou např. nevhodně navržené autentizační mechanizmy a z toho pramenící slabá ochrana hranice interní infrastruktury proti potenciálním útokům, které mohou přijít z vnějšku i z vnitřní sítě v rámci organizace, absence SIEM nástroje, který má na starosti vyhodnocování kritických bezpečnostních událostí a incidentů, určení technických rolí, které by byly i nezávislým orgánem vůči interním i externím administrátorům při vyhodnocování činnosti jednotlivých aktiv z pohledu bezpečnosti, nedostatečné

nasazení nástrojů, které mají zajišťovat ochranu vůči pokročilým malware hrozbám a „0-day" útokům, nesprávně nastavená pravidla emailové komunikace – scházejí nástroje, které budou detekovat pokročilé malware hrozby, absence interní dokumentace upravující nakládání s daty, zejména s těmi uloženými v e-mailové komunikaci – chybí tak jakákoli pravidla pro mazání, archivaci nebo uchovávání údajů či zasílání osobních údajů v rámci e-mailové komunikace. Dalším problémem je také nesprávné nakládání s informačními aktivy společnosti – chybí identifikace a definování kategorií těchto aktiv a jejich následné vyhodnocení z pohledu důvěrnosti, integrity a dostupnosti dat. Dalším problém je také problematika logování ve společnosti, tedy získávání, shromažďování a uchovávání informací o přístupech a nakládání s jednotlivými daty.

- **Kamerový systém je popsán, resp. zaznamenán nedostatečně** – častým nedostatkem bývá neúplná úprava, resp. evidence jednotlivých kamer, chybějící záznamy, které neobsahují účely specifikované pro jednotlivé kamery nebo jejich bližší specifikaci. Dalším problémem také často bývá absence jasně definované a nastavené správy a údržby kamerového systému (pravidelné prohlídky systému a jednotlivých kamer, servisní prohlídky apod.).
- **Chybí vnitropodniková či smluvní dokumentace** – v rámci společností jsou jen málokdy zakotvena základní pravidla pro nakládání s osobními dokumenty, e-mailovými schránkami, softwarem i hardwarem společnosti apod. Tato pravidla většinou ve společnosti fungují tzv. pouze na zvykovém právu, případně jsou řešeny ústně. Stejně tak byly zjištěny nedostatky spojené s nekompletní nebo zcela absentující dokumentací, zvláštně v rámci poskytování údajů třetím stranám (obchodním partnerům, v rámci skupin i do třetích zemí).
- **Procesy ve společnosti dosud nejsou upraveny** – ve společnosti nejsou upraveny a zakotveny procesy plnění práv subjektů a povinností správce.

S ohledem na výše uvedené je patrné, že samotná implementace GDPR, resp. rozsah porušení, kterého se může společnost dopustit, je velmi rozmanitý. Ačkoli se může jevit, že nedostatky v digitální oblasti jsou nejrozšířenější, neznamená to automaticky, že jsou také nejzávažnější. Za nejzávažnější jsou považována porušení základních zásad GDPR, které se promítají spíše v nesprávném právním nastavení systému ochrany osobních údajů ve společnosti, než s nastavením bezpečnosti dat. Výše uvedený seznam může být příkladným seznamem typizovaných pochybení společností, kdy objevení těchto porušení je vždy prvním krokem k správné implementaci GDPR. **Dalším neméně důležitým krokem však vždy musí být implementace těch správných a vhodných nápravných opatření.**

Autor: Mgr. Lucie Šimková (Jelínek & Partneři)

(www.epravo.cz 3. 4. 2018)

GDPR: jak efektivně implementovat za „pět minut dvanáct"?

Dne 25. 5. 2018 nabývá účinnosti nové evropské obecné nařízení o ochraně osobních údajů známé pod anglickou zkratkou GDPR. Podnikatelům, společnostem a ostatním správcům osobních údajů tak zbývá již pouze několik týdnů na přípravu a zajištění souladu.

I když značná část firem v tomto procesu už výrazně pokročila nebo je dokonce před jeho dokončením, stále existuje nezanedbatelné množství organizací, které jsou teprve na startu nebo těsně za ním.

Připravili jsme proto shrnutí našich zkušeností a doporučení z mnoha realizovaných GDPR projektů tak, aby většina běžných obchodních či výrobních firem, u kterých zpracování osobních údajů hraje pouze podpůrnou roli, byla schopna dosáhnout ve zbývajícím čase alespoň uspokojivé úrovně souladu s GDPR.

Mapování je základ

Prvním krokem přípravy na GDPR je identifikace a zmapování veškerých procesů zpracování osobních údajů, které ve firmě provádíte. Nemusí se jednat o žádné sofistikované postupy, ale v podstatě stačí zodpovězení základních „kriminalistických" otázek pro každé zpracování identifikované dle jeho účelu:

- kdo (jsme správce nebo zpracovatel),
- co (jaké údaje zpracováváme),
- proč (za jakým účelem a na základě jakého zákonného důvodu),
- o kom (koho se údaje týkají), komu (komu mohou být údaje zpřístupněny),
- kdy (jak dlouho údaje držíme) a
- jak (jak údaje zpracováváme a chráníme).

V optimálním případě by výstupem této mapovací fáze měl být přehled zpracování osobních údajů, který bude možné následně využít jako podklad pro záznamy o zpracování osobních údajů podle GDPR.

Provedení rozdílové analýzy

Pokud máte zmapovány procesy zpracování ve společnosti, přichází další krok spočívající v porovnání současného stavu se šesti povinnostmi každého správce osobních údajů dle GDPR.

Především je tak nutné prověřit, zda používáte pro dané zpracování správný zákonný důvod (zákonnost). Zvláštní pozornost je potřeba věnovat souhlasu s ohledem na zpřísnění požadavků pro jeho získání a udržení. Souhlas jako zákonný důvod zpracování doporučujeme využívat pouze tehdy, pokud skutečně nemůžete využít jiný zákonný důvod (plnění právní povinnosti, uzavření či plnění smlouvy nebo oprávněný zájem správce).

Po stanovení správného zákonného důvodu následuje prověření, zda veškeré údaje, které zpracováváte, jsou nezbytné pro legitimní a předem stanovený účel zpracování (omezení účelem), a zda je uchováváte pouze po nezbytnou dobu (minimalizace údajů a doby uchování). Je také nutné zabezpečit, abyste zpracovávali pouze přesné a podle potřeby aktualizované osobní údaje (přesnost).

Dále je potřeba podívat se na informace, které subjektům údajů o zpracování poskytujete a jakým způsobem budete reagovat na jejich související žádosti a práva a napomáhat jim při jejich výkonu (transparentnost a férovost). Ve většině případů stávající informace nebudou odpovídat požadavkům GDPR na obsah i formu. Obvykle ve firmách absentují také procesy, jak budou reagovat na žádosti subjektů.

Konečně je nutné zhodnotit rizikovost každého zpracování a přijmout a zdokumentovat odpovídající technická a organizační opatření k ochraně zpracování před neoprávněným přístupem či zpracováním a před náhodnou ztrátou, zničením nebo poškozením údajů (integrita a důvěrnost).

A konečně samotná implementace

Doporučujeme, abyste na základě zjištěných nedostatků stanovili konkrétní nápravná opatření zajišťující soulad s GDPR. S ohledem na čas je nutné identifikovat priority pro implementaci a přijmout odpovídající harmonogram.

V každém případě je možné předpokládat, že se nevyhnete následujícím v podstatě „standardním“ implementačním opatřením:

- vytvoření nebo aktualizace evidence zpracování (záznamů o zpracování),
- přijetí nové nebo revidované interní dokumentace, a to zejména v oblasti HR (vstupní dotazníky, pracovní smlouvy, směrnice pro nakládání s osobními údaji, informace pro zaměstnance),
- přijetí nové nebo revidované externí dokumentace (oznámení o zpracování, souhlasy s přímým marketingem, obchodní podmínky),
- revize a doplnění smluv se zpracovateli (typicky externí mzdová účtárna nebo bezpečnostní agentura či poskytovatelé benefitů),
- provedení základní rizikové analýzy (vč. zhodnocení případné potřeby jmenování pověřence nebo detailnějšího posuzování vlivu zpracování),
- dokumentace technických a organizačních opatření k zabezpečení zpracování vč. nastavení interních procesů (reakce na žádosti a výkon práv, ohlašování a dokumentace incidentů atd.),
- školení a testování zaměstnanců.

Tento výčet není vyčerpávající a představuje pouze standardní základní „implementační balíček“. Konkrétní rozsah implementačních opatření se bude vždy lišit zejména podle rozsahu, povahy, kontextu a účelu zpracování. V každém případě se jedná o obvyklé minimum, které z velké části můžete řešit ve zbývajícím čase.

I pokud se případně nepodaří vše stihnout do účinnosti GDPR, není nutné, abyste propadali beznaději a pasivně čekali na masivní pokutu! Je zcela legitimní očekávat, že zmapování zpracování, částečná implementace priorit a reálný harmonogram pro zbývající opatření budou vždy zohledněny v případě kontroly a měly by vás uchránit před uložením nějaké zásadní sankce.

Autor: Radek Matouš (Dvořák Hager & Partners)

(www.epravo.cz 25. 4. 2018)

GDPR: nastane s nástupem nové regulace nedostatek pověřenců?

S účinností obecného nařízení o ochraně osobních údajů[1] („GDPR“[2] nebo „nařízení“) vznikne správcům i zpracovatelům osobních údajů řada nových povinností. Jednou z nich je dle nového právního rámce stanovená povinnost jmenovat pověřence pro ochranu osobních údajů („pověřenec“ nebo „DPO“[3]), která slouží zejména ke kontrole odpovědnosti. Pověřenec by měl správcům (zpracovatelům) mimo jiné usnadnit dodržování souladu jejich činnosti s GDPR, avšak nový institut s sebou přináší řadu nezodpovězených otázek týkajících se jmenování, certifikace či odpovědnosti DPO, které správce tíží v návaznosti na blížící se účinnost nařízení (25. 5. 2018).

Pohled do historie a evropská vodítka

Někteří správci usazení v EU jsou s institutem pověřence víceméně již sžiti, jak uvádíme níže, ale pro velkou část z nich bude tento institut něčím novým, s čím doposud zkušenost nemají. Funkce pověřence byla v zemích EU zavedena směrnicí 95/46/ES[4] („**směrnice**“). Česká republika se vydala především cestou oznamovací/registrační povinnosti a nevyužila možnost spočívající v zakotvení v právním řádu osoby pověřené ochranou osobních údajů. Pověřenec ustanovený na základě směrnice měl, obdobně jako ten dle GDPR, nezávislým způsobem zajistit interní uplatňování vnitrostátních předpisů přijatých k provedení směrnice a také vést seznam zpracování prováděných správcem. Dle informací z roku 2005 obsažených ve stanovisku[5] pracovní skupiny zřízené podle článku 29 směrnice („**WP29**“) pouze pět členských států EU využilo výjimku z notifikace, a zavedlo tak předpoklady pro výkon funkce pověřence.[6] Některé státy jako Německo podmínky výkonu funkce DPO upravily detailněji a stanovily v národní legislativě kupříkladu rozdílné podmínky povinného jmenování pro subjekty veřejného práva a pro subjekty soukromoprávní.[7] Ze států nám právní tradicí bližších zavedlo v roce 2013 funkci pověřence např. také Slovensko, které na rozdíl od jiných států umožnilo výkon této funkce svěřit pouze fyzickým osobám.[8]

Současná právní úprava DPO vychází z dosavadních zkušeností jednotlivých členských států EU, které popisuje výše zmíněné stanovisko pracovní skupiny WP29. Nicméně i přes veškeré dosavadní zkušenosti s tímto institutem nařízení ne zcela jasně a zřetelně upravuje některé podmínky, resp. požadavky pro výkon této funkce. Proto vydala pracovní skupina WP29 dne 13. 12. 2016 (revize ze dne 5. 4. 2017) pokyny/vodítka („**pokyny**“), které mají zejména ujasnit podmínky jmenování, postavení a plnění úkolů pověřenců. Postavení DPO, požadavkům na ně či plnění jejich úkolů se podrobněji věnujeme v našem článku *Pověřenec pro osobní údaje dle GDPR: koho a jak pověřit?.*[9]

Jmenování DPO

Povinnost jmenovat pověřence se sice od května 2018 nebude vztahovat na všechny správce a zpracovatele, ale samotná pracovní skupina WP29 i v případě subjektů, na které povinnost jmenování nedopadá, doporučuje též dobrovolné jmenování, jelikož existence pověřence může snížit riziko porušení pravidel stanovených nařízením.

Funkci pověřence může vykonávat interní zaměstnanec správce či zpracovatele nebo externí subjekt na základě smlouvy o poskytování služeb. V obou případech musí pověřenec splňovat všechny požadavky na něho kladené a zároveň musí být chráněn proti nezákonnému ukončení smlouvy o poskytování služeb nebo nezákonnému propuštění. DPO se zejména nesmí v souvislosti se svou činností dostat do střetu zájmů. Pověřenec smí pro správce, resp. zpracovatele plnit i jiné úkoly za podmínky, že nepovedou ke střetu zájmů. Kvůli hrozbě střetu zájmů nesmí pověřenec v organizaci určovat účely a prostředky zpracování osobních údajů. Ke střetu zájmů může dojít i v případě, kdy by měl pověřenec zastupovat správce nebo zpracovatele v soudním či obdobném řízení v případech týkajících se ochrany osobních údajů. S touto podmínkou úzce souvisí ustanovení článku 38 odst. 3 GDPR, dle kterého pověřenec vykonává svou činnost nezávisle a s dostatečnou

[1] Nařízení Evropského parlamentu a Rady č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[2] General Data Protection Regulation.
[3] Data Protection Officer.
[4] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[5] Stanovisko pracovní skupiny zřízené podle článku 29 směrnice o povinnosti informovat národní dozorové orgány, nejlepší použití výjimek a zjednodušení a o roli inspektorů ochrany osobních údajů v Evropské unii. 10211/05/EN, WP 106.
[6] Německo, Nizozemí, Švédsko, Lucembursko a Francie.
[7] V Německu je každý subjekt s více než čtyřmi osobami zapojenými do automatizovaného zpracování údajů povinen jmenovat inspektora ochrany osobních údajů. Každý veřejný subjekt má bez výjimky povinnost jmenovat inspektora ochrany osobních údajů.
[8] § 27 odst. 3 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov; Zodpovednou osobou môže byť len fyzická osoba, ktorá má spôsobilosť na právne úkony v plnom rozsahu, je bezúhonná a má platné potvrdenie úradu o absolvovaní skúšky podľa § 24.
[9] Pověřenec pro osobní údaje dle GDPR: koho a jak pověřit?, dostupné na www, k dispozici zde.