3. 4. 2018

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

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 úrovní** – 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 informováni, 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.**

Mgr. Lucie Šimková

Advokátní kancelář JELÍNEK & Partneři s.r.o.

Pardubice - Dražkovice 181
533 33 Pardubice - Dražkovice

Velké náměstí 1
500 03 Hradec Králové

Truhlářská 1108/3
110 00 Praha 1

Tel.: +420 466 310 691
Fax: +420 466 310 691

gsm: +420 724 794 986
e-mail: advokati@advokatijelinek.cz

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- 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
- DEAL MONITOR
- DEAL MONITOR
- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie