Květen 2017

Škola ochrany osobních údajů

advokátní kanceláře Balcar, Polanský & Spol. s.r.o.

Nařízení EP a Rady (EU) 2016/679 z 27. dubna 2016, tzv. Všeobecné nařízení o ochraně údajů („Nařízení") zrušilo směrnici 95/46/ES („Směrnice"), která je nyní transformována do českého právního řádu zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Nařízení vstoupí v účinnost dnem 25. května 2018, kdy se stane přímo účinným rovněž v České republice a dotkne se všech, kteří osobní údaje zpracovávají, jakož i fyzických osob, jejichž osobní údaje jsou předmětem zpracování, tedy téměř každého.

Vzhledem k dosud nejvýznamnější legislativní změně evropského rozměru v oblasti ochrany osobních údajů Vám s týdenní frekvencí přinášíme pravidelné informace pro snadnější a efektivnější orientaci v množství povinností, které Nařízení přináší.

Pokud si přejete odebírat Školu osobních údajů přímo do Vaší e-mailové schránky, prosím přihlaste se na adrese office@bapol.cz, popř. na tel. čísle +420 251 009 111.

Lekce 10 z 16

Bezpečnost osobních údajů a porušení jejich ochrany

V textu se dozvíte:

Důležité změny

- Správci budou mít v případě porušení ochrany osobních údajů dvojí oznamovací povinnost - jednak vůči dozorovému úřadu, jednak vůči subjektům údajů;
- Správci budou povinni vést evidenci porušení ochrany osobních údajů.

Compliance: Akční plán

- Správci a rovněž zpracovatelé musí provést vhodná bezpečnostní opatření na ochranu dat při zpracování;
- Pro tento účel je nezbytné důkladně posoudit okolnosti zpracování, a to ve spolupráci s IT techniky (např. pro účely zavedení šifrování údajů);
- Doporučuje se zavést interní směrnice pro případ zjištění porušení ochrany údajů;
- Doporučuje se zvážit možnost pojištění následků případného porušení ochrany osobních údajů;
- Pokud smlouvy s dodavateli zahrnují zpracování osobních údajů (např. výplatní pásky, účetnictví), měly by obsahovat odpovědnost za bezpečnost osobních údajů[1].

[1] Smlouva o zpracování je brána za součást bezpečnostních opatření.

Bezpečnost osobních údajů

Nařízení stanoví minimální standard ochrany osobních údajů při jejich zpracování prostřednictvím několika institutů, resp. opatření, která je správce povinen přijmout[2]. Z Nařízením sledovaného záměru je zřejmé, že hlavním účelem nové legislativy upravující zpracování osobních údajů je zajištění jejich bezpečnosti při zpracování a minimalizace rizik – nejen před následky lidského jednání (úmyslného či nedbalostního, interního u správce či zpracovatele nebo vnějšího, mimo tyto subjekty), ale i přírodních sil nebo selhání techniky - spojených s různými operacemi zpracování.

Nařízení upravuje povinnosti související s bezpečností osobních údajů tak, že správce (a také zpracovatel) je povinen provést vhodná technická a organizační opatření, aby zajistil náležitou úroveň bezpečnosti, včetně důvěrnosti, odpovídající tomuto riziku. Tato opatření mohou zahrnovat také:

- pseudonymizaci a šifrování osobních údajů;
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Nařízení uvádí výše uvedená bezpečnostní opatření pouze jako příklady, tj. správce může stanovit i jiná vhodnější opatření k zajištění bezpečnosti údajů, podle svých specifických podmínek. Nařízení stanoví, jakého stavu musí správci a zpracovatelé docílit, ale nikoliv již jakými prostředky. Tato opatření však musí být zavedena s ohledem na:

- *aktuální stav techniky* – za účelem zjištění, jaké možnosti ochrany osobních údajů v době stanovování bezpečnostních opatření existují, je vhodné, aby správce konzultoval aktuální prostředky ochrany s IT specialisty. Opatření musí vykazovat náležitou odbornou úroveň. Je vhodné je poté v pravidelných intervalech obnovovat; pokud by se totiž v průběhu zpracování osobních údajů úroveň poznatků o způsobech ochrany zlepšila, nemusel by mít správce z důvodu zastaralosti ochranných systémů zajištěn soulad s Nařízením;
- *náklady na provedení opatření* – při přijímání konkrétních opatření zvažuje správce i jejich nákladnost. Argumentem není, že bezpečnostní opatření nebyla přijata vzhledem k jejich finanční, personální či časové náročnosti;
- *povahu, rozsah, kontext a účely zpracování* – při určovaní, jaká bezpečnostní opatření správce přijme, je třeba samozřejmě důkladně zvážit všechny okolnosti zpracování osobních údajů v době, kdy ke zpracování dochází; rovněž tyto okolnosti je potřeba průběžně přehodnocovat vzhledem k měnícím se podmínkám zpracování;
- *různě závažná rizika pro práva a svobody fyzických osob* – jde o důležitý aspekt zpracování, přičemž od správce se vyžaduje, aby provedl vyhodnocení jakýchkoliv možných bezpečnostních rizik spojených se zpracováním, která by mohla mít negativní dopad na práva a svobody fyzických osob. Toto posouzení rizik by mělo být provedeno zejména s ohledem na rizika vyplývající z automatizovaného zpracování (např. hackerské útoky, selhání IT techniky, neoprávněné nebo neodborné zásahy třetích osob do procesu zpracování) a s ohledem na rizika spojená s prostředím, ve kterém se data nacházejí (např. zabezpečení budov a prostor, protipožární ochrana, dostupnost serverů a jiných úložišť dat apod.). Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování,

[2] Jedná se zejména o povinnost vést záznamy o činnostech zpracování, povinnost přijmout přiměřená technická a organizační opatření, oznamovací povinnost v případě porušení ochrany osobních údajů, posouzení vlivu na ochranu osobních údajů, předchozí konzultace s dozorovým úřadem a pod.

neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim[3].

Z uvedeného je zřejmé, že to, jaká konkrétní bezpečnostní opatření správce v konečném důsledku přijme, by mělo být výsledkem důkladného posouzení okolností zpracování v konkrétních podmínkách každého správce nebo zpracovatele.

Účinností Nařízení nastává podstatná změna v tom, že správci již nebudou muset vypracovat bezpečnostní projekty či dokumentaci[4], jak tomu bylo doposud. Místo toho bude potřeba – pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob - provést před zpracováním posouzení vlivu ochrany údajů (*„privacy impact assessment"*, *„PIA"*), případně požádat dozorový úřad o konzultaci podle čl. 35 a 36 Nařízení. Tato povinnost se bude aplikovat ve specifických případech, např. při rozsáhlém systematickém monitorování veřejně přístupných míst, pokud bude správce ve velkém rozsahu zpracovávat citlivé údaje nebo osobní údaje týkající se rozsudků v trestních věcech, při profilování či automatizovaném rozhodování apod.

Pro účely zajištění a prokázání přijetí vhodných bezpečnostních opatření je možné, aby správce přistoupil k dodržování schváleného kodexu chování[5] nebo schváleného mechanismu pro vydávání osvědčení[6]. Správce je rovněž povinen zajistit, aby každá fyzická osoba jednající na základě pověření správce, která má přístup k osobním údajům (momentálně tzv. odpovědná osoba) zpracovávala tyto údaje pouze na základě pokynů správce, s výjimkou případů, kdy je po ní zpracování vyžadováno podle unijního práva nebo práva členského státu.

Podstatnou povinností správce a zpracovatele je pak důsledná kontrola plnění přijatých opatření a povinností odpovědných osob. Samotná PIA či konzultace Úřadu a následné přijetí bezpečnostních technických a organizačních opatření tedy nebude postačovat.[7]

Oznamování porušení zabezpečení osobních údajů

Jakkoliv odpovědně přistupuje správce k ochraně osobních údajů, které zpracovává, nebude zřejmě možné zcela vyloučit riziko porušení jejich zabezpečení (*„data breach"*). Takovým porušením se rozumí zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim[8].

Nařízení upravuje v souvislosti s porušením ochrany osobních údajů dva druhy oznamovací povinnosti správců:

a) *Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu*

V případě porušení zabezpečení osobních údajů je správce povinen v první řadě ohlásit tuto skutečnost dozorovému úřadu příslušnému podle čl. 55 Nařízení. Toto ohlášení je třeba učinit bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl. Pokud není ohlášení učiněno ve stanovené době, musí být současně s ním uvedeny důvody tohoto zpoždění.

Pokud není správce schopen z objektivních příčin poskytnout dozorovému úřadu informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

---

[3] Čl. 32 odst. 2 Nařízení.

[4] § 13 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

[5] Čl. 40 Nařízení.

[6] Čl. 42 Nařízení.

[7] Kontrola nemusí být specializovaná na ochranu osobních údajů, může být součástí uplatňování práva a povinnosti vedoucích pracovníků kontrolovat v rámci pracovně-právních vztahů práci podřízených zaměstnanců. Možností je také využití již standardních automatizovaných prostředků, např. tzv. logů (záznamů o přístupu konkrétní osoby do systému).

[8] Čl. 32 odst. 2 Nařízení.

Ohlášení musí obsahovat přinejmenším:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Správce není povinen ohlásit porušení dozorovému úřadu, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

b) Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

Pokud dojde k porušení zabezpečení osobních údajů, které bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, je správce povinen toto porušení bez zbytečného odkladu oznámit subjektu údajů.

V oznámení správce za použití jasných a jednoduchých jazykových prostředků popíše povahu porušení zabezpečení osobních údajů a uvede přinejmenším tyto informace a opatření:

- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů; a
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Také v tomto případě Nařízení upravuje výjimku, kdy správce není povinen porušení oznámit subjektu údajů. Oznámení se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

- správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
- vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil.

Zdokumentování porušení zabezpečení osobních údajů

Kromě výše uvedené oznamovací povinnosti je správce povinen také interně zdokumentovat každý případ porušení zabezpečení osobních údajů včetně skutečností s porušením zabezpečení osobních údajů spojených, jeho následky a opatření přijatá k nápravě a tyto dokumenty uchovávat.

Mimo to je správce povinen splnit také určitý komunikační (tj. dokumentační standard při ohlašování porušení dozorovému úřadu a oznamování subjektům údajů (náležitosti těchto oznámení viz výše).

Co dále

Správci i zpracovatelé by měli před účinností Nařízení prověřit svá dosavadní interní technická a organizační opatření z hlediska nových požadavků, vyhodnotit znovu míru rizik s ohledem na stávající stav techniky, nákladovost opatření a povahu zpracovávaných osobních údajů, aktualizovat svá dosavadní bezpečnostní opatření a kontrolní a odpovědnostní mechanismy, zajistit řádnou evidenci a postupy pro včasné hlášení případných bezpečnostních incidentů. Shledají-li vysoké riziko pro práva a svobody fyzických osob, měli by provést PIA, příp. konzultovat Úřad. Uvedené kroky by měli také být schopni zpětně doložit a zdůvodnit v zájmu průkaznosti a své liberace z případné odpovědnosti jak soukromoprávní (za újmu subjektů údajů či dotčených osob), tak veřejnoprávní (za správní delikt) či trestněprávní odpovědnosti (např. trestný čin neoprávněného nakládání s osobními údaji).

Další informace

Recitály 83 - 94

Články 32 - 34

Kontaktní osoba

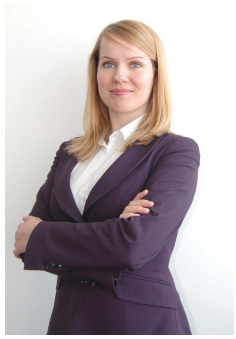
Pro další informace prosím kontaktujte:

Česká republika:

JUDr. Jaroslav Srb
Advokát

Tel.: +420 220 251 111
Mobil: +420 731 609 510

jaroslav.srb@bapol.cz



Slovensko:

JUDr. Helga Maďarová, CIPP/E
Advokátka | Certified Intl. Privacy Professional/Europe

Tel.: +421 220 251 311
Mobil: +421 917 092 076

helga.madarova@bapol.sk