Máj 2017

Škola ochrany osobných údajov

advokátskej kancelárie Balcar, Polanský & Spol. s.r.o.

Nariadenie EP a Rady (EÚ) 2016/679 z 27. apríla 2016, tzv. Všeobecné nariadenie o ochrane údajov („Nariadenie") zrušilo smernicu 95/46/ES („Smernica"), ktorá je momentálne pretransformovaná aj do slovenského právneho poriadku prostredníctvom zákona č. 122/2013 Z. z. o ochrane osobných údajov. Nariadenie nadobudne účinnosť dňom 25. mája 2018, kedy bude priamo účinné aj na Slovensku a dotkne sa všetkých, ktorí osobné údaje spracúvajú, ako aj fyzických osôb, ktorých osobné údaje sú predmetom spracúvania, teda takmer každého.

Vzhľadom na doposiaľ najvýznamnejšiu legislatívnu zmenu európskeho rozmeru v oblasti ochrany osobných údajov Vám na týždennej báze prinášame pravidelné informácie, aby ste sa mohli ľahšie a efektívnejšie zorientovať v spleti povinností, ktoré Nariadenie prináša.

Ak si prajete odoberať Školu osobných údajov priamo do Vašej e-mailovej schránky, prosím prihláste sa na odber na adrese office@bapol.sk, prípadne na tel. čísle +421 220 251 311.

Lekcia 10 z 16

Bezpečnosť osobných údajov a porušenie ich ochrany

V texte sa dozviete:

Dôležité zmeny

- Prevádzkovatelia budú mať dvojakú oznamovaciu povinnosť v prípade porušenia ochrany osobných údajov, a to jednak voči dozornému úradu, a tiež voči dotknutým osobám;
- Prevádzkovatelia budú povinní viesť evidenciu porušení ochrany osobných údajov.

Compliance: Akčný plán

- Prevádzkovatelia aj sprostredkovatelia musia zaviesť vhodné bezpečnostné opatrenia na ochranu dát pri spracúvaní;
- Za týmto účelom je potrebné dôsledne posúdiť okolností spracúvania, a to v spolupráci s IT technikmi (napr. pre účely zavedenia šifrovania údajov);
- Odporúča sa zaviesť interné smernice pre prípad zistenia porušenia ochrany údajov;
- Odporúča sa zvážiť poistenie následkov prípadného porušenia ochrany osobných údajov;
- Zmluvy s dodávateľmi, ak zahŕňajú spracúvanie osobných údajov (napr. výplatné pásky, účtovníctvo), by mali obsahovať zodpovednosť za bezpečnosť osobných údajov[1].

[1] Zmluva o spracúvaní sa považuje za súčasť bezpečnostných opatrení.

Bezpečnosť osobných údajov

Nariadenie stanovuje minimálny štandard ochrany osobných údajov pri ich spracúvaní prostredníctvom niekoľkých inštitútov, resp. opatrení, ktoré je prevádzkovateľ povinný prijať[2]. Z Nariadením sledovaného zámeru je zrejmé, že hlavným účelom novej legislatívy upravujúcej spracúvanie osobných údajov je zabezpečenie ich bezpečnosti pri spracúvaní a minimalizácia rizík – nielen pred následkami ľudského konania (úmyselného, nedbanlivostného, interného u prevádzkovateľa či sprostredkovateľa alebo vonkajšieho, mimo týchto subjektov), ale i prírodných síl alebo zlyhania techniky – spojených s rôznymi spracovateľskými operáciami.

Nariadenie upravuje povinnosti prevádzkovateľa súvisiace s bezpečnosťou osobných údajov tak, že prevádzkovateľ (a tiež sprostredkovateľ) je povinný prijať vhodné technické a organizačné opatrenia s cieľom zaistiť náležitú úroveň bezpečnosti, vrátane dôvernosti, zodpovedajúcu tomuto riziku. Tieto opatrenia môžu zahŕňať aj:

- pseudonymizáciu a šifrovanie osobných údajov;
- schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Nariadenie uvádza vyššie uvedené bezpečnostné opatrenia výlučne ako príklady, t.j. prevádzkovateľ môže určiť aj iné vhodnejšie opatrenia na zabezpečenie bezpečnosti údajov, podľa jeho špecifických podmienok. Nariadenie stanovuje, aký stav musia prevádzkovatelia a sprostredkovatelia docieliť, ale nie, akými prostriedkami. Tieto opatrenia však musí zaviesť so zreteľom na:

- *najnovšie poznatky techniky* – za účelom zistenia, aké možnosti ochrany osobných údajov v momente určovania bezpečnostných opatrení existujú, je vhodné, aby prevádzkovateľ konzultoval aktuálne prostriedky ochrany s IT špecialistami. Opatrenia musia vykazovať náležitú odbornú úroveň. Tieto je potom vhodné v pravidelných intervaloch obnovovať; ak by sa totiž v priebehu spracúvania osobných údajov úroveň poznatkov o prostriedkoch ochrany rozvinula, prevádzkovateľ by z dôvodu obsolétnosti ochranných systémov nemusel mať zabezpečený súlad s Nariadením;
- *náklady na vykonanie opatrení* – pri prijímaní konkrétnych opatrení prevádzkovateľ zvažuje aj ich nákladovosť. Argumentom nie je, že bezpečnostné opatrenia neboli prijaté vzhľadom na ich finančnú, personálnu či časovú náročnosť;
- *povahu, rozsah, kontext a účely spracúvania* – pri určovaní, aké bezpečnostné opatrenia prevádzkovateľ príjme, samozrejme musí dôkladne zvážiť všetky okolnosti spracúvania osobných údajov v čase, kedy k spracúvaniu dochádza; tieto okolnosti je potrebné priebežne prehodnocovať vzhľadom na meniace sa podmienky spracúvania;
- *riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb* – ide o dôležitý aspekt spracúvania, pričom od prevádzkovateľa sa vyžaduje, aby urobil vyhodnotenie akýchkoľvek možných bezpečnostných rizík spojených so spracúvaním, ktoré by mohli mať negatívny dopad na práva a slobody fyzických osôb. Toto posúdenie rizík by sa malo vykonať najmä s ohľadom na riziká vyplývajúce z automatizovaného spracúvania (napr. hackerské útoky, zlyhanie IT techniky, neoprávnené alebo neodborné zásahy tretích

[2] Ide najmä o povinnosť viesť záznamy o spracovateľských činnostiach, povinnosť prijať primerané technické a organizačné opatrenia, oznamovaciu povinnosť v prípade porušenia ochrany osobných údajov, posúdenie vplyvu na ochranu osobných údajov; predchádzajúce konzultácie s dozorným orgánom a pod.

osôb do spracovateľského procesu), ako aj s ohľadom na riziká spojené s okolím, v ktorom sa dáta nachádzajú (napr. zabezpečenie budov a priestorov, protipožiarna ochrana, dostupnosť serverov a iných úložísk dát a pod.). Pri posudzovaní primeranej úrovne bezpečnosti sa totiž prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom[3].

Z uvedeného je zrejmé, že to, aké konkrétne bezpečnostné opatrenia prevádzkovateľ v konečnom dôsledku prijme, by malo byť výsledkom dôsledného posúdenia okolností spracúvania v konkrétnych podmienkach toho – ktorého prevádzkovateľa alebo sprostredkovateľa.

Účinnosťou Nariadenia nastáva podstatná zmena v tom, že prevádzkovatelia už nebudú musieť vypracovať bezpečnostné projekty[4] alebo dokumentáciu, ako tomu bolo doteraz. Namiesto toho bude potrebné – ak je pravdepodobné, že určitý druh spracovania bude mať za následok vysoké riziko pre práva a slobody fyzických osôb – vykonať pred spracúvaním posúdenie vplyvu ochrany údajov (*„privacy impact assessment", „PIA"*), prípadne požiadať Úrad o konzultáciu podľa čl. 35 a 36 Nariadenia. Táto povinnosť sa bude aplikovať v špecifických prípadoch, napr. pri systematickom monitorovaní verejne prístupných miest vo veľkom rozsahu, ak prevádzkovateľ bude spracúvať osobné údaje o uznanie viny za trestné činy a priestupky, profilovanie či automatizované individuálne rozhodovanie a pod.

Pre účely zabezpečenia a preukázania prijatia vhodných bezpečnostných opatrení je možné, aby prevádzkovateľ pristúpil k dodržiavaniu schváleného kódexu správania[5] alebo schváleného certifikačného mechanizmu[6]. Tiež, prevádzkovateľ je povinný zabezpečiť, aby každá fyzická osoba konajúca na základe poverenia prevádzkovateľa, ktorá má prístup k osobným údajom (momentálne tzv. oprávnená osoba), spracúvala tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to od nej vyžaduje podľa práva Únie alebo práva členského štátu.

Podstatnou povinnosťou prevádzkovateľa a sprostredkovateľa bude dôsledná kontrola plnenia prijatých opatrení a povinností zodpovedných osôb. Samotná PIA či konzultácia Úradu a následné prijatie bezpečnostných technických a organizačných opatrení teda nebude postačovať.[7]

Oznámenie porušenia ochrany osobných údajov

Akokoľvek zodpovedne prevádzkovateľ pristupuje k ochrane osobných údajov, ktoré spracúva, zrejme nebude možné úplne vylúčiť riziko porušenia ochrany osobných údajov (*„data breach"*). Takým porušením sa rozumie najmä náhodné alebo nezákonné zničenie, strata, zmena, neoprávnené poskytnutie osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k takýmto údajom[8].

Nariadenie upravuje v súvislosti s porušením ochrany osobných údajov dva druhy oznamovacej povinnosti prevádzkovateľov:

a) Oznámenie porušenia príslušnému dozornému orgánu

V prípade porušenia ochrany osobných údajov je prevádzkovateľ v prvom rade povinný oznámiť túto skutočnosť dozornému orgánu príslušnému podľa článku 55 Nariadenia. Toto

[3] Čl. 32 ods. 2 Nariadenia.

[4] § 20 zákona č. 122/2013 Z.z. o ochrane osobných údajov.

[5] Čl. 40 Nariadenia.

[6] Čl. 42 Nariadenia.

[7] Kontrola nemusí byť špecializovaná na ochranu osobných údajov, môže byť súčasťou uplatňovania práv a povinností vedúcich zamestnancov kontrolovať v rámci pracovno-právnych vzťahov prácu podriadených zamestnancov. Možnosťou je tiež využitie už štandardných automatizovaných prostriedkov, napr. tzv. logov (záznam o prístupe konkrétnej osoby do systému).

[8] Čl. 32 ods. 2 Nariadenia.

oznámenie je potrebné vykonať bez zbytočného odkladu, avšak podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti prevádzkovateľ dozvedel. Ak oznámenie nebolo predložené v stanovenej dobe, pripojí sa k nemu zdôvodnenie tohto omeškania.

Ak prevádzkovateľ nie je schopný z objektívnych príčin poskytnúť dozornému orgánu informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

Oznámenie musí obsahovať aspoň:

- opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
- opis pravdepodobných následkov porušenia ochrany osobných údajov;
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Prevádzkovateľ nie je povinný oznamovať porušenie dozornému orgánu, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

b) *Oznámenie porušenia ochrany osobných údajov dotknutej osobe*

Ak dôjde k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ je povinný oznámiť porušenie ochrany osobných údajov aj dotknutej osobe. Toto oznámenie je povinný vykonať bez zbytočného odkladu.

V oznámení prevádzkovateľ uvedie jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň tieto informácie a opatrenia:

- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
- opis pravdepodobných následkov porušenia ochrany osobných údajov; a
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Aj v tomto prípade Nariadenie upravuje výnimku, kedy prevádzkovateľ nie je povinný porušenie oznamovať dotknutej osobe. Oznámenie sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:

- prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie;
- prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky;
- by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, dozorný orgán môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil.

Zdokumentovanie porušenia ochrany osobných údajov

Okrem uvedenej oznamovacej povinnosti je prevádzkovateľ povinný aj interne zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu, a tieto dokumenty uchovávať.

Okrem toho prevádzkovateľ musí splniť aj určitý komunikačný (t.j. dokumentačný) štandard pri oznamovaní porušenia dozornému orgánu a dotknutým osobám (náležitosti takých oznámení viď vyššie).

Čo ďalej

Prevádzkovatelia a sprostredkovatelia by mali pred účinnosťou Nariadenia preveriť svoje doterajšie interné technické a organizačné opatrenia z hľadiska nových požiadaviek, vyhodnotiť mieru rizík s ohľadom na súčasný stav techniky, nákladovosť opatrení a povahu spracovávaných osobných údajov, aktualizovať svoje súčasné bezpečnostné opatrenia a kontrolné a zodpovednostné mechanizmy, zabezpečiť riadnu evidenciu a postupy pre včasné hlásenie prípadných bezpečnostných incidentov. Ak zistia vysoké riziko pre práva a slobody fyzických osôb, je potrebné vykonať PIA, prípadne konzultovať Úrad. Uvedené kroky by mali byť tiež schopní spätne doložiť a zdôvodniť v záujme preukázateľnosti a svojej liberácie z prípadnej súkromnoprávnej zodpovednosti (za škodu spôsobenú dotknutej osobe), ako aj verejnoprávnej (za správny delikt) či trestnoprávnej (napr. trestný čin neoprávneného nakladania s osobnými údajmi).

Ďalšie informácie

Recitály 83 - 94

Články 32 - 34

Kontaktná osoba

Pre ďalšie informácie prosím kontaktujte:

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

Česká republika:

JUDr. Jaroslav Srb
Advokát

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

jaroslav.srb@bapol.cz