

Bird & Bird

Oznamovanie porušení osobných údajov (tzv. bezpečnostných incidentov) a udeľovanie sankcií podľa GDPR

Zhrnutie

Obsah

1.	Východiská oznamovacej povinnosti	3
2.	Oznámenie dozornému orgánu	5
3.	Oznámenie dotknutej osobe	6
4.	Výnimky z oznamovacej povinnosti	7
5.	Zdokumentovanie	7
6.	Ďalšie oznamovacie povinnosti	8
7.	Princípy ukladania sankcií	8
8.	Faktory ovplyvňujúce výšku pokuty	9

1. Východiská oznamovacej povinnosti

Nariadenie Európskeho parlamentu a Rady č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov ("**GDPR**") zavádza notifikačnú povinnosť informovať o porušení ochrany osobných údajov (tzv. bezpečnostných incidentoch), a to jednak dozorný orgán, ako aj dotknuté osoby o porušení ochrany osobných údajov (za splnenia nižšie popísaných zákonných podmienok).

*„Porušenie ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie **k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov**, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.*"¹

Spôsoby porušenia ochrany osobných údajov môžeme podľa ich charakteru rozdeliť nasledovne:²

- **Narušenie dôvernosti** - prípady neoprávneného alebo náhodného zverejnenia alebo prístupu k osobným údajom.
- **Narušenie integrity** - prípady neoprávnenej alebo náhodnej zmeny osobných údajov.
- **Narušenie dostupnosti** – prípady náhodnej alebo neoprávnenej straty prístupu k osobným údajom alebo ich zničenie (vrátane straty dekrypčného kľúča). Strata dostupnosti môže byť trvalá (strata údajov bez existencie zálohy), alebo dočasná (v dôsledku výpadku elektrického prúdu, útoku Denial of Service – DoS, atď.)

Všetky spôsoby porušenia ochrany osobných údajov je potrebné zdokumentovať³, avšak nie všetky je prevádzkovateľ povinný ohlásiť. Každý konkrétny prípad je preto nevyhnutné osobitne posúdiť.

Základným hodnotiacim kritériom je existencia rizika, či pravdepodobne dôjde k porušeniu práv a slobôd fyzických osôb. Ak áno, tak je potrebné vždy urobiť oznámenie (1) príslušnému dozornému orgánu, a v niektorých prípadoch aj (2) dotknutej osobe.

Oznámenie príslušnému dozornému orgánu:

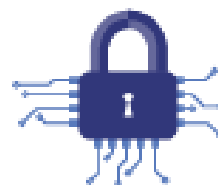
- V prípade porušenia ochrany osobných údajov, ktoré **pravdepodobne povedie k riziku** pre práva a slobody fyzických osôb.
- Časový faktor - bez zbytočného odkladu a podľa možnosti najneskôr do **72 hodín** po tom, čo sa o tejto skutočnosti dozvedel

Oznámenie aj dotknutej osobe:

- V prípade porušenia ochrany osobných údajov, ktoré **pravdepodobne povedie k vysokému riziku** pre práva a slobody fyzických osôb.
- Časový faktor - **bez zbytočného odkladu**

Príklad:

Ak by v prípade výpadku elektrického prúdu v nemocnici, ktorá spracúvala osobné údaje, sa tieto stali dočasne nedostupné, tak existuje reálne riziko, že pravdepodobne dôjde k porušeniu práv a slobôd fyzických osôb, nakoľko bez týchto údajov napríklad nebudú môcť byť vykonané niektoré vyšetrenia. Na druhú stranu, ak by obdobná situácia nastala v spoločnosti, ktorá spracúva osobné údaje klientov (mená



¹ Čl. 4 (12) GDPR

² Usmernenie Pracovnej skupiny podľa článku 29 (WP29) č. 3/2014

³ Čl. 33 (5) GDPR, bližšie pozri kapitolu č. 5

a emailové adresy) pre marketingové účely, a tieto budú dočasne nedostupné v dôsledku výpadku elektrického prúdu, tak riziko že dôjde k porušeniu práv a slobôd fyzických osôb prakticky neexistuje.

Európska agentúra pre bezpečnosť sietí a informácií (ENISA) vypracovala odporúčania pre metodiku posudzovania bezpečnostných incidentov, ktorú môžu prevádzkovatelia aj sprostredkovatelia použiť pri tvorbe interných systémov na riadenie porušení ochrany osobných údajov ako aj posudzovania ich rizík.⁴

Medzi hodnotiace kritéria pri posudzovaní rizika patrí:

Typ porušenia

- Druh porušenia ochrany osobných údajov zohráva významnú úlohu pri posudzovaní rizík, napr. zničenie osobných údajov sa bude inak posudzovať ako ich odcudzenie.

Povaha, citlivosť a rozsah osobných údajov

- Nielen typ porušenia, ale aj typ samotných osobných údajov je dôležitý pri hodnotení závažnosti konkrétneho bezpečnostného incidentu. V zásade platí, že finančné údaje (ako údaje o platobnej karte), alebo zdravotné záznamy sú spôsobilé privodiť väčšiu ujmu ako napríklad údaj o adrese pobytu osoby, alebo verejne dostupné údaje. Pričom riziko sa zvyšuje pri množstve druhov a kombinácií týchto údajov. Každý prípad je však potrebné posudzovať osobitne.

Závažnosť dopadu na dotknuté osoby

- V rámci každého bezpečnostného incidentu je potrebné posúdiť, či a do akej miery má dopad na konkrétne dotknuté osoby, napr. môže dôjsť ku krádežiam identity alebo podvodu, k fyzickej alebo psychickej ujme, či poškodeniu reputácie. Dopad na dotknuté osoby je potrebné posudzovať z dlhodobého aj krátkodobého hľadiska. Naopak znížený, alebo minimálny dopad môže mať situácia, kde sa osobné údaje pošlú omylom inému oddeleniu v rámci spoločnosti (prípadne spoľahlivému a dôveryhodnému obchodnému partnerovi), tento chybný adresát sa okamžite o tejto skutočnosti dozvie a všetky údaje natrvalo zničí. Uvedený prípad nemusí vytvoriť žiadne riziko pre práva a slobody fyzických osôb, a preto ho ani nemusí byť nevyhnutné oznamovať dozornému orgánu a dotknutým osobám.

Osobitné charakteristiky dotknutej osoby a prevádzkovateľa

- Osobitný prístup je potrebné dodržiavať jednak voči deťom a iným zraniteľným osobám, ktoré sú vo väčšom riziku (napr. adoptované dieťa sa porušením ochrany osobných údajov dozvie inak neprístupné informácie o svojom biologickom rodičovi), ale aj voči prevádzkovateľovi (napríklad zdravotnícke zariadenia, ktoré spracúvajú vysoko citlivé údaje).

Náročnosť identifikácie dotknutých osôb

- Dôležitým faktorom je aj stupeň náročnosti, akým je možné pomocou získaných osobných údajov priamo alebo nepriamo identifikovať konkrétnu osobu, t.j. či sú údaje pseudonymizované, vysoko účinne kryptované, alebo naopak nie sú vôbec zabezpečené a akým spôsobom sa dajú kombinovať s verejnými údajmi.

Počet dotknutých osôb

- Všeobecne platí, že čím vyšší počet dotknutých osôb, tým je bezpečnostný incident závažnejší. Toto však nevyklučuje prípad, že aj keď bude dotknutý len jeden subjekt, tak môže ísť o vysoko závažný bezpečnostný incident.

⁴ ENISA, Odporúčania pre metodiku hodnotenia závažnosti porušenia osobných údajov, Dostupné online: <https://www.enisa.europa.eu/publications/dbn-severity>

2. Oznámenie dozornému orgánu

V prípade porušenia ochrany osobných údajov je prevádzkovateľ povinný bez zbytočného odkladu a podľa možnosti **najneskôr do 72 hodín od okamihu, čo sa o tejto skutočnosti dozvedel**, oznámiť porušenie ochrany osobných údajov dozornému orgánu.⁵

Okamihom, kedy sa prevádzkovateľ mohol o porušení ochrany osobných údajov dozvedieť je okamih, kedy prevádzkovateľ **s primeraným stupňom istoty** zistil, že došlo k bezpečnostnému incidentu, ktorý viedol k ohrozeniu osobných údajov.

Po tom ako sa prevádzkovateľ dozvie o potencionálnom bezpečnostnom incidente, tak má istý časový priestor na zbežné prešetrenie toho, či k porušeniu ochrany osobných údajov došlo alebo nie. V tomto štádiu ešte nehovoríme, že prevádzkovateľ sa o bezpečnostnom incidente dozvedel až do okamihu, kým sa s primeraným stupňom istoty neustáli v presvedčení, že k porušeniu ochrany osobných údajov došlo. Následné a detailné vyšetrovanie bezpečnostného incidentu môže pokračovať po vykonaní oznámenia dozornému orgánu.

V prípade, že k bezpečnostnému incidentu dôjde na strane **sprostredkovateľa**, tento je povinný prevádzkovateľa o tejto skutočnosti bez zbytočného odkladu informovať. Prevádzkovateľ sa v tomto prípade dozvedel o danom bezpečnostnom incidente momentom, keď mu to sprostredkovateľ oznámi. Vzťah medzi sprostredkovateľom a prevádzkovateľom funguje na tom princípe, že sprostredkovateľ koná pri spracúvaní osobných údajov na základe a podľa pokynov prevádzkovateľa, preto by aj v zmluve medzi prevádzkovateľom a sprostredkovateľom mala byť stanovená tiež povinnosť sprostredkovateľa pomáhať prevádzkovateľovi zabezpečiť plnenie oznamovacích povinností s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi.⁶

V tejto súvislosti je tiež prípustné, aby sám sprostredkovateľ vykonal oznámenie dozornému orgánu, ak sa na tom prostredníctvom zmluvy dohodne s prevádzkovateľom (za oznamovanie a splnenie všetkých povinností je však stále zo zákona povinný prevádzkovateľ).

Jedným z hlavných dôvodov oznamovania je minimalizovanie škody vzniknutej dotknutým osobám.⁷ Oznámenie dozornému orgánu, preto musí obsahovať nasledovné informácie:

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

V prípade, že všetky uvedené informácie nie je schopný prevádzkovateľ poskytnúť okamžite, tak existuje aj možnosť ich oznámiť po fázach, čím sa zachová zákonná povinnosť prevádzkovateľa informovať dozorný orgán do



⁵ Čl. 33 (1) GDPR

⁶ Čl. 28 (3)f GDPR

⁷ Recitál 85 GDPR

72 hodín.⁸ Uvedené nevylučuje skutočnosť, že sám dozorný orgán si môže vyžiadať dodatočné informácie. Rovnako je možné, že vyšetrovanie bude vyžadovať dlhší čas, v takom prípade má prevádzkovateľ možnosť ohlásiť bezpečnostný incident len čiastočne a pripojiť k oznámeniu zdôvodnenie omeškania.⁹ Dozorný orgán zároveň môže pomôcť prevádzkovateľovi v posúdení rizika, resp. splnenia zákonných podmienok na oznámenie aj voči dotknutým osobám.

V zmysle uvedeného je vhodné, aby prevádzkovateľ mal vytvorený systém interných predpisov, ktoré budú upravovať uvedené procesy, najmä:

- **Detekciu bezpečnostných incidentov (spracúvanie logov, toku dát a pod.)**
- **Informácie týkajúce sa všetkých bezpečnostných incidentov by mali smerovať k zodpovednej osobe alebo osobám, pre účely efektívneho posúdenia rizika (pravdepodobnosť rizika/vysokého rizika).**
- **Oznamovanie dozornému orgánu a dotknutým osobám.**
- **Vyšetrenie a náprava prípadných bezpečnostných incidentov.**

3. Oznámenie dotknutej osobe

Ako už bolo zmienené vyššie, povinnosť oznámiť bezpečnostný incident dotknutej osobe nastáva až v prípade existencie pravdepodobnosti **vysokého** rizika pre práva a slobody fyzických osôb, na rozdiel od povinnosti notifikovať dozorný orgán kde sa uplatňuje podmienka existencie pravdepodobnosti "len" rizika pre práva a slobody fyzických osôb.

V praxi tak môžeme očakávať, že nie všetky bezpečnostné incidenty, ktoré budú ohlásené dozornému orgánu, budú ohlásené aj konkrétnym fyzickým osobám.

Dotknuté osoby by mali byť kontaktované priamo a bez zbytočného odkladu. Za primeranú formu sa považujú individuálne správy poslané priamo konkrétnej osobe (prípustné sú formy poštovej komunikácie, emailu, SMS, priamej správy), avšak nie oznamy v rámci regulárnych marketingových správ a aktualizácií (newsletter).



⁸ Čl. 33 (4) GDPR

⁹ Čl. 33 (1) GDPR

4. Výnimky z oznamovacej povinnosti

Bezpečnostné incidenty, pri ktorých **nie je pravdepodobné, že dané porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb sa nemusia oznamovať.**

Môže ísť napríklad o údaje, ktoré sú verejne prístupné. Rovnako v prípade, ak budú osobné údaje zašifrované najmodernejšou technológiou a takým zložitým algoritmom, že ich nie je možné dešifrovať neautorizovanou osobou (t.j. bezpečnostný kľúč zostal nedotknutý), tak riziko pre dotknuté osoby nie je veľké, a preto nebude potrebné vykonať oznámenie voči nim ani dozornému orgánu (za predpokladu, že prevádzkovateľ disponuje zálohou príslušných osobných údajov a tento bezpečnostný incident nepredstavuje žiadne riziko pre práva a slobody fyzických osôb). Usmernenie Pracovnej skupiny WP 29 však aj v tomto prípade upozorňuje, že pravdepodobnosť rizika môže po určitom čase predsa len nastať (napr. sa stanú dostupnými nové dešifrovacie technológie), a preto bude potrebné toto riziko opätovne potrebné posúdiť.¹⁰

GDPR stanovuje presne tri prípady kedy nie je potrebné oznámiť bezpečnostný incident dotknutému subjektu (to však nevyklučuje povinnosť oznámiť bezpečnostný incident dozornému orgánu):

- a prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia, a to najmä tie, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie;
- b prevádzkovateľ okamžite prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky (nebude existovať);
- c by to **vyžadovalo neprimerané úsilie** (napríklad by došlo k vyhoreniu skladu, kde boli osobné údaje uskladnené len v písomnej podobe a tieto písomnosti boli zničené). V takom prípade dôjde namiesto toho k informovaniu verejnosti (napr. prostredníctvom prominentných elektronických alebo printových médií) alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom. V princípe však platí, že oznámenie na webovej stránke prevádzkovateľa, alebo len v elektronických médiách sa nepovažuje za dostačujúcu v porovnaní s individuálnym oznámením konkrétnym dotknutým osobám.

V každom z uvedených prípadov musí byť prevádzkovateľ schopný dozornému orgánu riadne preukázať, že jeden z týchto dôvodov nastal.

Vo všeobecnosti však platí princíp, že za oznámenie bezpečnostného incidentu, ktorý sa nemusel ohlásiť (nenastalo žiadne riziko) dozornému orgánu, sa neukladá sankcia, ale za neoznámenie bezpečnostného incidentu, ktorý sa mal ohlásiť (existencia rizika) sa sankcia ukladá.

5. Zdokumentovanie

"Prevádzkovateľ zdokumentuje **každý prípad porušenia ochrany osobných údajov** vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu. Uvedená dokumentácia musí umožniť dozorným orgánom overiť súlad s týmto článkom." ¹¹

V zmysle uvedeného je Prevádzkovateľ povinný zdokumentovať všetky prípady porušenia ochrany osobných údajov, a to v internom registri porušení, bez ohľadu na to, či tieto prípady ohlasoval, alebo nie. Zriadenie osobitného registra pre porušenia sa však nevyžaduje. Prevádzkovateľ teda môže prípady porušenia zaznamenávať v registri, ktorý vedie podľa čl. 30 GDPR, s tým že v tomto registri musia byť zaznamenané všetky potrebné informácie - príčiny, čo sa stalo, identifikácia dotknutých osobných údajov, dopady porušenia ochrany týchto údajov, ako aj spôsoby nápravy.

¹⁰ Porovnaj Usmernenie Pracovnej skupiny podľa článku 29 (WP29) č. 10/2017, pričom opačný názor je vyslovený v predchádzajúcom Usmernení Pracovnej skupiny podľa článku 29 (WP29) č. 3/2014, podľa ktorého aj takéto bezpečnostné incidenty bolo potrebné nahlásiť dozorným orgánom podľa čl. 4 (1-2) Nariadenia Komisie EÚ č. 611/2013

¹¹ Čl. 33 (5) GDPR

Ak v danom prípade nebolo porušenie ochrany osobných údajov oznámené dozornému orgánu, alebo dotknutej osobe, tak je nevyhnutné zdokumentovať dôvod a podklady na takéto rozhodnutie. Toto obdobie platí aj v prípade oneskoreného oznámenia.

Nesplnenie povinnosti riadne zdokumentovať porušenie môže viesť k uloženiu správnej pokuty.¹² Je preto žiaduce, aby prevádzkovateľ aj sprostredkovateľ osobných údajov mali vytvorené interné procesy detekcie bezpečnostných incidentov, hodnotenia ich rizík, oznamovania, obnovy osobných údajov, ale aj dokumentovanie týchto bezpečnostných incidentov.

6. Ďalšie oznamovacie povinnosti

Pre úplnosť ešte uvádzame, že niektoré subjekty môžu mať popri oznamovacej povinnosti podľa GDPR, oznamovaciu povinnosť na základe týchto predpisov:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (**Nariadenie eIDAS**)
- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 z 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (**Smernica NIS**)
- Smernica Európskeho parlamentu a Rady (EÚ) 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb.

7. Princípy ukladania sankcií

Nariadenie GDPR v čl. 58 (2) stanovuje podrobný zoznam právomocí dozorných orgánov pre prípad porušenia ochrany osobných údajov. Tieto právomoci však príslušné orgány nesmú udeľovať svojvoľne, práve naopak musia sa striktne riadiť princípmi spravodlivého a primeraného postihovania, medzi ktoré patrí:

Princíp ukladania rovnocenných sankcií

Táto podmienka ukladania sankcií jednak zdôrazňuje rovnaký stupeň ochrany a postihovania porušenia ochrany osobných údajov v jednotlivých členských štátoch EÚ, ako aj nadväzuje na princíp cezhraničnej kooperácie dozorných orgánov.



Pričom aj keď právne systémy niektorých členských štátov (napr. Dánsko) neumožňujú ukladanie správnych pokút stanovených v tomto nariadení, tak uplatňované sankcie v týchto štátoch má mať rovnocenný účinok ako správne pokuty ukladané dozornými orgánmi podľa GDPR.¹³

Princíp efektívnosti sankcií

V rámci zachovania efektivity sankčných mechanizmov sa v zmysle GDPR uplatňuje zásada, že dozorný orgán musí zabezpečiť v každom jednotlivom prípade účinné, primerané a odrádzajúce sankcie.¹⁴

¹² Čl. 83 GDPR

¹³ Recitál 151 GDPR

¹⁴ Čl. 83 (1) GDPR

Princíp individuálneho posudzovania

Správne pokuty sa v závislosti od okolností každého jednotlivého prípadu ukladajú popri opatreniach alebo namiesto nich. Pri rozhodovaní o uložení správnej pokuty a jej výške sa v každom jednotlivom prípade musia náležite zohľadniť početné faktory (uvedené nižšie).

Princíp aktívnej súčinnosti dozorných orgánov

Harmonizovaný prístup k správnym pokutám v oblasti ochrany osobných údajov vyžaduje aktívnu účasť a výmenu informácií medzi dozornými orgánmi navzájom, ako aj s Európskou Komisiou, čo pomôže aj k lepšej predvídateľnosti rozsahu ukladaných sankcií v jednotlivých členských štátoch.

8. Faktory ovplyvňujúce výšku pokuty

a) Povaha, závažnosť a trvanie porušenia,

Konkrétne porušenia ochrany osobných údajov nemajú fixne stanovené výšky pokút, ale vymedzenia ohraničujúce rozsah možných sankcií, pričom stropy sankcií sú rôzne (10-20 miliónov EUR). V prípade menej závažného porušenia, alebo ak by pravdepodobne uložená pokuta predstavovala pre prevádzkovateľa (sprostredkovateľa) - fyzickú osobu neprimeranú záťaž, možno namiesto uloženia pokuty **udelieť aj napomenutie**.

Pri udeľovaní sankcií sa ďalej zohľadňuje povaha, rozsah alebo účel dotknutého spracúvania, ako aj počet dotknutých osôb, na ktoré malo vplyv. Rovnako je potrebné posúdiť aj rozsah škody, ktorú dotknuté osoby utrpeli.

Riziko pre práva a slobody fyzických osôb s rôznym stupňom pravdepodobnosti a závažnosti môže viesť až k ujme na zdraví, majetkovej alebo nemajetkovej ujme, a to najmä ak spracúvanie, resp. porušenie ochrany osobných údajov viedlo k diskriminácii, krádeži totožnosti alebo podvodu, finančnej strate, poškodeniu dobrého mena, strate dôvernosti osobných údajov chránených profesijným tajomstvom, neoprávnenej reverznej pseudonymizácii alebo akémukoľvek inému závažnému hospodárskemu alebo sociálnemu znevýhodneniu.¹⁵

Bez ohľadu na uvedené, uloženie pokuty nezávisí len od schopnosti dozorného orgánu preukázať príčinnú súvislosť medzi porušením ochrany osobných údajov a prípadnou majetkovou ujmov.



¹⁵ Recitál 75 GDPR

b) Úmyselný alebo nebanlivostný charakter porušenia;

Vo všeobecnosti sú úmyselné porušenia považované za závažnejšie (napr. pozmenenie osobných údajov pre účely zlepšenia štatistiky, alebo predaj osobných údajov pre účely marketingu).

c) Akékoľvek kroky, ktoré prevádzkovateľ alebo sprostredkovateľ podnikol s cieľom zmierniť škodu, ktorú dotknuté osoby utrpeli;

Prevádzkovateľ a sprostredkovateľ sú povinní vykonať všetky opatrenia vedúce k zabezpečeniu dostatočnej ochrany osobných údajov. V prípade, že k uvedenému porušeniu aj napriek tomu dôjde, tak spôsob a rýchlosť konania, ktoré prevádzkovateľ vykonal (nevykonal) budú mať dôležitý význam na to, ako sa naň bude prihliadať zo strany dozorného orgánu. Pozitívny prístup môže zahŕňať napríklad promptné kontaktovanie všetkých dotknutých prevádzkovateľov alebo sprostredkovateľov, alebo ľubovoľné iné efektívne konanie, ktoré zastaví, resp. minimalizuje negatívny dopad porušenia ochrany osobných údajov.

d) Miera zodpovednosti prevádzkovateľa alebo sprostredkovateľa so zreteľom na technické a organizačné opatrenia, ktoré prijali;

Prevádzkovateľ je povinný v čase spracúvania osobných údajov prijať primerané (1) technické a (2) organizačné opatrenia na všetkých úrovniach organizácie, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začleniť do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.¹⁶

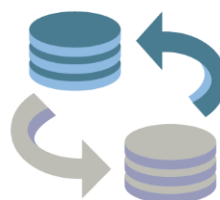
Nie však len prevádzkovateľ, ale aj sprostredkovateľ je povinný prijať so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia. Tieto opatrenia zahŕňajú napríklad pseudonymizáciu a šifrovanie osobných údajov, proces pravidelného testovania opatrení atď.¹⁷

e) Akékoľvek relevantné predchádzajúce porušenia zo strany prevádzkovateľa alebo sprostredkovateľa;

Dozorný orgán posudzuje všetky predchádzajúce porušenia ochrany osobných údajov zo strany porušovateľa. Nie je pritom rozhodujúce, či boli tieto porušenia rovnakého druhu, prípadne za akých okolností k nim došlo. Samozrejme tieto otázky zohrávajú úlohu v tom, ako sa k nim dozorný orgán postaví, no posúdiť musí všetky porušenia subjektu. Pričom práve tento súvis so súčasným porušením ochrany osobných údajov bude rozhodujúci pri udeľovaní sankcie.

f) Miera spolupráce s dozorným orgánom pri náprave porušenia;

Intenzita spolupráce sprostredkovateľa alebo prevádzkovateľa s dozorným orgánom pri náprave porušenia a zmiernení možných nepriaznivých dôsledkov porušenia môže mať významný vplyv na to, ako dozorný orgán posúdi konkrétne porušenie. Hoci žiadny právny predpis neurčuje akým spôsobom má dozorný orgán na túto spoluprácu prihliadať, v prípade že porušovateľ bude konať správnym spôsobom počas vyšetřovania bezpečnostného incidentu dozorným orgánom a preukáže, že vyvinul maximálne úsilie na minimalizovanie dopadu na práva fyzických osôb, tak je možno očakávať, že dozorný orgán zmierni výšku prípadnej sankcie.



g) Kategórie osobných údajov, ktorých sa porušenie týka;

Dozorný orgán pristupuje s väčšou vážnosťou k prípadom porušenia ochrany osobných údajov spadajúcich do osobitných kategórií osobných údajov.

Ide napríklad o spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory,

¹⁶ Čl. 25 (1) GDPR

¹⁷ Čl. 25 (1) GDPR

náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

h) Spôsob, akým sa dozorný orgán o porušení dozvedel, a najmä to, či prevádzkovateľ alebo sprostredkovateľ porušenie oznámili, a ak áno, v akom rozsahu;

V prípade, ak porušovateľ o porušení vedel a snažil sa ho úmyselne zatajiť, tak dozorný orgán len ťažko môže zmierniť prípadnú sankciu. Naopak, pokiaľ porušovateľ promptne reagoval, splnil si všetky svoje oznamovacie povinnosti a spolupracoval s dozorným orgánom, tento bude brať ohľad na daný prístup prevádzkovateľa a môže aj so zreteľom na iné okolnosti znížiť prípadnú sankciu.

i) Ak boli predtým voči dotknutému prevádzkovateľovi alebo sprostredkovateľovi v rovnakej veci prijaté opatrenia uvedené v článku 58 ods. 2, splnenie uvedených opatrení;

Toto kritérium má len pripomenúť dozornému orgánu, aby vzal na zreteľ opatrenia voči danému subjektu z minulosti s ohľadom na rovnaký predmet. Pri opakovanom porušení prevádzkovateľom alebo spracovateľom, dozorný orgán vykoná dôkladné šetrenie a posúdi novú výšku "recidívnej" sankcie, ktorá môže byť vyššia ako tá predchádzajúca.

j) Dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;

Dodržiavanie schválených kódexov môže byť jedným z dôležitých nástrojov prevádzkovateľa, ktorými preukáže súlad svojho konania so zákonnými povinnosťami. Navyše schválené kódexy správania obsahujú mechanizmy, ktoré umožňujú subjektu vykonávať povinné monitorovanie dodržiavania zákona zo strany prevádzkovateľov alebo sprostredkovateľov, ktorí sa rozhodli uplatňovať ho. Po podrobnom posúdení konkrétneho prípadu a sankčných mechanizmov subjektu v jeho vlastnom kódexe, dozorný orgán môže rozhodnúť, že ďalšia sankcia ani nemusí byť potrebná a žiaduca (prípadne iba v zníženej forme).

k) Akékoľvek iné priťažujúce alebo poľahčujúce okolnosti prípadu.

Do tejto kategórie radíme najmä akékoľvek získané finančné výhody alebo straty, ktorým sa zabránilo, priamo alebo nepriamo v súvislosti s porušením. V tejto súvislosti možno len poukázať na fakt, že informácia o výnose získanom v dôsledku porušenia ochrany osobných údajov je jedným z významných faktorov, ktoré ovplyvnia výšku udeľovanej sankcie.

"Poskytnutie predmetných informácií nemá charakter poskytnutia právnych služieb, resp. právneho poradenstva zo strany advokátskej kancelárie Bird & Bird ani neformuluje právny názor advokátskej kancelárie na uvedenú problematiku. Predmetné informácie podávajú sumár najkľúčovejších aspektov v zmysle Usmernenia o oznamovaní porušení ochrany osobných údajov a v zmysle Usmernenia o uplatňovaní a stanovení správnych pokút podľa Nariadenia 2016/679 (GDPR) vypracovaných Pracovnou skupinou podľa článku 29 na ochranu osôb pri spracúvaní osobných údajov zriadenou podľa Smernice 95/46/EC zo dňa 3.10.2017."



Contacts

Vojtěch Chloupek

Partner

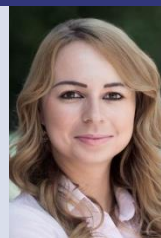
Tel: +420 226 030 518
vojtech.chloupek@twobirds.com



Katarína Pfeffer

Advokátka

Tel: +421 232 332 800
katarina.pfeffer@twobirds.com



Robert Čuperka

Advokátsky koncipient

Tel: +421 232 332 800
robert.cuperka@twobirds.com



twobirds.com

Aarhus & Abu Dhabi & Bratislava & Brusel & Budapešť & Kodaň & Dubaj & Düsseldorf & Frankfurt & Haag & Hamburg & Helsinki & Hong Kong & Londýn & Luxemburg & Lyon & Madrid & Miláno & Mníchov & Paríž & Peking & Praha & Rím & Šanghai & Singapur & Štokholm & Sydney & Varšava

Bird & Bird je medzinárodná advokátska kancelária skladajúca sa z Bird & Bird LLP a jej pobočiek a pridružených zastúpení.

Bird & Bird LLP je registrované v Anglicku a Walse pod registračným číslom OC340318 a je regulované SRA – Regulačnou autoritou. Jej sídlom a miestom podnikania je 12 New Fetter Lane, Londýn, EC4A 1JP. Zoznam členov skupiny Bird & Bird LLP a nečlenov, ktorí sú vymenovaní za partnerov a ich príslušné odborné kvalifikácie, sú k dispozícii k nahliadnutiu na tejto adrese.