PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

18/SK

WP250rev.01

Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679

Prijaté 3. októbra 2017

naposledy revidované a prijaté utorok 6. februára 2018

Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom na ochranu údajov a súkromia. Jej úlohy sú uvedené v článku 30 smernice 95/46/ES a článku 15 smernice 2002/58/ES.

Sekretariát zabezpečuje riaditeľstvo C (základné práva a občianstvo Únie) Európskej komisie, generálne riaditeľstvo pre spravodlivosť, B-1049 Brusel, Belgicko, úrad č. MO-59 02/013.

Webové sídlo: http://ec.europa.eu/justice/data-protection/index_sk.htm

PRACOVNÁ SKUPINA PRE OCHRANU JEDNOTLIVCOV SO ZRETEĽOM NA SPRACOVANIE OSOBNÝCH ÚDAJOV,

ktorá bola zriadená smernicou Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995,

so zreteľom na články 29 a 30 uvedenej smernice,

so zreteľom na svoj rokovací poriadok,

PRIJALA TIETO USMERNENIA:

OBSAH

ÚVOD

Všeobecným nariadením o ochrane údajov (GDPR) sa zavádza požiadavka týkajúca sa porušenia ochrany osobných údajov (ďalej len „porušenie“), ktoré sa má oznámiť príslušnému vnútroštátnemu dozornému orgánu[1] (alebo v prípade cezhraničného porušenia vedúcemu orgánu) a v určitých prípadoch oznámiť porušenie jednotlivcom, ktorých osobné údaje boli porušením dotknuté.

Pre niektoré organizácie, ako sú poskytovatelia verejne dostupných elektronických komunikačných služieb (ako sú špecifikované v smernici 2009/136/ES a v nariadení (EÚ) č. 611/2013), v súčasnosti existujú povinnosti oznamovať prípady porušenia[2]. Existujú aj niektoré členské štáty EÚ, ktoré už majú svoje vlastné vnútroštátne povinnosti oznamovania porušení. To môže zahŕňať povinnosť oznamovať porušenia týkajúce sa kategórií prevádzkovateľov okrem poskytovateľov verejne dostupných elektronických komunikačných služieb (napríklad v Nemecku a Taliansku), alebo povinnosť hlásiť všetky porušenia týkajúce sa osobných údajov (napríklad v Holandsku). Ostatné členské štáty môžu mať príslušné kódexy postupov (napríklad v Írsku[3]). Zatiaľ čo viaceré orgány EÚ na ochranu údajov v súčasnosti podnecujú prevádzkovateľov, aby oznamovali porušenia, smernica 95/46/ES o ochrane údajov[4], ktorú nahrádza GDPR, neobsahuje konkrétnu povinnosť oznamovať porušenie, a preto bude takáto požiadavka pre mnohé organizácie nová. V GDPR sa teraz zavádza povinnosť oznamovania pre všetkých prevádzkovateľov, s výnimkou prípadov, kedy je nepravdepodobné, že by porušenie mohlo viesť k ohrozeniu práv a slobôd jednotlivcov[5]. Aj sprostredkovatelia zohrávajú dôležitú úlohu a musia oznámiť akékoľvek porušenie svojmu prevádzkovateľovi[6].

Pracovná skupina zriadená podľa článku 29 (ďalej len „pracovná skupina podľa článku 29“) sa domnieva, že nová oznamovacia povinnosť má niekoľko výhod. Pri oznamovaní dozornému orgánu môžu prevádzkovatelia získať radu, či majú byť dotknuté osoby informované. Dozorný orgán môže samozrejme nariadiť prevádzkovateľovi, aby o týchto porušeniach informoval tieto osoby[7]. Oznámenie porušenia jednotlivcom umožňuje prevádzkovateľovi poskytnúť informácie o rizikách, ktoré vznikli v dôsledku porušenia, a o krokoch, ktoré môžu jednotlivci podniknúť, aby sa chránili pred jeho možnými následkami. Zmyslom každého plánu reakcie na porušenie by mala byť ochrana jednotlivcov a ich osobných údajov. Oznámenie porušenia by sa preto malo považovať za nástroj zlepšujúci súlad v súvislosti s ochranou osobných údajov. Zároveň treba poznamenať, že neoznámenie porušenia jednotlivcovi alebo dozornému orgánu môže znamenať, že podľa článku 83 sa na prevádzkovateľa vzťahuje prípadná sankcia.

Prevádzkovatelia a sprostredkovatelia sa preto vyzývajú, aby vopred naplánovali a zaviedli postupy na odhalenie porušenia a rýchle zabránenie jeho šíreniu, posúdili riziko pre jednotlivcov[8], a potom určili, či je potrebné informovať príslušný dozorný orgán, a aby v prípade potreby oznámili porušenie dotknutým osobám. Oznámenie dozornému orgánu by malo byť súčasťou tohto plánu reakcie na incidenty.

---

1 Pozri článok 4 ods. 21 GDPR.

2 Pozri https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32009L0136 a https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32013R0611.

3 Pozri https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

4 Pozri https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:31995L0046.

5 Práva zakotvené v Charte základných práv EÚ, ktorá je k dispozícii na https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:12012P/TXT.

6 Pozri článok 33 ods. 2. To je koncepčne podobné s článkom 5 nariadenia (EÚ) č. 611/2013, v ktorom sa stanovuje, že poskytovateľ, ktorý je zmluvne zaviazaný poskytovať časti elektronickej komunikačnej služby (bez priameho zmluvného vzťahu s účastníkmi), je povinný oznámiť zmluvnému poskytovateľovi prípady porušenia ochrany osobných údajov.

7 Pozri článok 34 ods. 4 a článok 58 ods. 2 písm. e).

8 To možno zabezpečiť na základe požiadavky na monitorovanie a preskúmanie posúdenia vplyvu na ochranu údajov, ktoré sa vyžaduje na spracovateľské operácie, ktoré by mohli predstavovať vysoké riziko pre práva a slobody fyzických osôb (článok 35 ods. 1 a článok 11).

GDPR obsahuje ustanovenia o tom, kedy je potrebné oznámiť porušenie a komu, ako aj aké informácie by sa mali poskytnúť ako súčasť oznámenia. Informácie požadované pre oznámenie môžu byť poskytnuté vo viacerých etapách, prevádzkovatelia by však v prípade akéhokoľvek porušenia mali konať včas.

Pracovná skupina podľa článku 29 vo svojom stanovisku 03/2014 k oznámeniu porušenia ochrany osobných údajov[9] poskytla prevádzkovateľom usmernenie s cieľom pomôcť im pri rozhodovaní o tom, či v prípade porušenia informovať dotknutú osobu. Obsahom stanoviska bolo posúdenie povinnosti poskytovateľov elektronickej komunikácie v súvislosti so smernicou 2002/58/ES a boli v ňom uvedené príklady z viacerých sektorov v kontexte vtedajšieho návrhu GDPR, ako aj osvedčené postupy pre všetkých prevádzkovateľov.

V týchto usmerneniach sa vysvetľujú požiadavky na povinné oznamovanie a nahlasovanie porušenia GDPR a niektoré opatrenia, ktoré môžu prevádzkovatelia a sprostredkovatelia prijať na splnenie týchto nových povinností. Uvádzajú sa v nich aj príklady rôznych typov porušení a to, kto by mal byť v rôznych scenároch informovaný.

I. Oznámenie porušenia ochrany osobných údajov podľa GDPR

A. Základné bezpečnostné hľadiská

Jednou z požiadaviek GDPR je, aby sa prostredníctvom primeraných technických a organizačných opatrení osobné údaje spracúvali spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením[10].

V GDPR sa preto vyžaduje, aby prevádzkovatelia aj sprostredkovatelia zaviedli primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú riziku, ktorému sú vystavené spracúvané osobné údaje. Mali by brať do úvahy najnovšie poznatky, náklady na vykonanie opatrení a povahu, rozsah, kontext a účely spracúvania, ako aj riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb[11]. V GDPR sa okrem toho vyžaduje, aby sa prijali všetky primerané technické ochranné a organizačné opatrenia na bezodkladné zistenie, či došlo k porušeniu, na základe čoho sa následne určí, či sa vykoná oznamovacia povinnosť[12].

Kľúčovým prvkom akejkoľvek politiky ochrany údajov je teda schopnosť zabrániť porušovaniu, pokiaľ je to možné, a ak k nemu napriek tomu dôjde, včas naň reagovať.

B. Čo je porušenie ochrany osobných údajov?

1. Vymedzenie pojmu

Na to, aby sa prevádzkovateľ mohol pokúsiť riešiť porušenie by mal byť schopný ho najskôr rozpoznať. V GDPR sa „porušenie ochrany osobných údajov“ vymedzuje v článku 4 ods. 12 ako:

> „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.“

[9] Pozri stanovisko 03/2014 k oznámeniu porušenia ochrany osobných údajov http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[10] Pozri článok 5 ods. 1 písm. f) a článok 32.

[11] Článok 32, Pozri aj odôvodnenie 83.

[12] Pozri odôvodnenie 87.

Význam pojmu „zničenie“ osobných údajov by mal byť úplne jasný: ide o situáciu, kedy údaje už neexistujú alebo už neexistujú vo forme, ktorá je pre prevádzkovateľa užitočná. Význam pojmu „poškodenie“ by mal byť tiež pomerne jasný: ide o situáciu, kedy boli osobné údaje zmenené, poškodené, alebo už nie sú úplné. Pokiaľ ide o „stratu“ osobných údajov, malo by sa to chápať tak, že údaje ešte môžu existovať, ale prevádzkovateľ stratil kontrolu nad týmito údajmi alebo prístup k nim, alebo ich už nemá k dispozícii. Nakoniec, neoprávnené alebo nezákonné spracúvanie môže zahŕňať poskytnutie osobných údajov (alebo prístupu k týmto údajom) príjemcom, ktorí nie sú oprávnení prijímať údaje (alebo k nim pristupovať), alebo akúkoľvek inú formu spracúvania, ktorou sa porušuje GDPR.

Príklad

Príkladom straty osobných údajov môže byť situácia, v ktorej je zariadenie obsahujúce kópiu zákazníckej databázy prevádzkovateľa stratené alebo ukradnuté. Ďalším príkladom straty môže byť situácia, v ktorej jediná kópia súboru osobných údajov bola zašifrovaná prostredníctvom softvéru ransomware alebo bola zašifrovaná prevádzkovateľom pomocou kľúča, ktorý už prevádzkovateľ nemá k dispozícii.

Malo by byť jasné, že porušenie je typ bezpečnostného incidentu. Ako však uvádza v článku 4 ods. 12, GDPR sa uplatňuje iba ak došlo k porušeniu ochrany osobných údajov. Dôsledkom takéhoto porušenia je, že prevádzkovateľ nebude schopný zabezpečiť dodržiavanie zásad súvisiacich so spracúvaním osobných údajov, ako sa uvádza v článku 5 GDPR. To zdôrazňuje rozdiel medzi bezpečnostným incidentom a porušením ochrany osobných údajov – v zásade, zatiaľ čo všetky porušenia ochrany osobných údajov sú bezpečnostnými incidentmi, nie všetky bezpečnostné incidenty sú nevyhnutne porušeniami ochrany osobných údajov[13].

Potenciálne nepriaznivé dôsledky porušenia na jednotlivcov sú uvedené ďalej.

2. Typy porušenia ochrany osobných údajov

Pracovná skupina podľa článku 29 vo svojom stanovisku 03/2014 k oznámeniu porušenia vysvetľuje, že porušenia možno kategorizovať podľa týchto troch všeobecne známych zásad bezpečnosti informácií[14]:

- „porušenie dôvernosti“ – keď dôjde k neoprávnenému alebo náhodnému poskytnutiu osobných údajov alebo prístupu k osobným údajom,
- „porušenie integrity“ – keď dôjde k neoprávnenej alebo náhodnej zmene osobných údajov,
- „porušenie dostupnosti“ – keď dôjde k náhodnej alebo neoprávnenej strate prístupu[15] alebo k zničeniu osobných údajov.

Okrem toho treba poznamenať, že v závislosti od okolností sa porušenie môže týkať dôvernosti, integrity a dostupnosti osobných údajov súčasne, ako aj akejkoľvek ich kombinácie.

---

13 Treba poznamenať, že bezpečnostný incident nie je obmedzený na modely ohrozenia, pri ktorých je organizácia napadnutá z vonkajšieho zdroja, ale zahŕňa aj prípady vnútorného spracúvania, ktoré porušujú bezpečnostné zásady.

14 Pozri stanovisko 03/2014.

15 Je všeobecne známe, že „prístup“ je v podstate súčasťou „dostupnosti“. Pozri napríklad NIST SP800-53rev4, kde sa „dostupnosť“ vymedzuje ako: „zabezpečenie včasného a spoľahlivého prístupu k informáciám a ich využitia,“ k dispozícii na adrese http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. V CNSSI-4009 sa uvádza aj: „včasný a spoľahlivý prístup k dátovým a informačným službám pre autorizovaných používateľov.“ Pozri https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. V ISO/IEC 27000:2016 sa „dostupnosť“ vymedzuje aj ako „vlastnosť charakterizovaná prístupnosťou informácií a ich použiteľnosťou na požiadanie oprávneného subjektu“: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Zatiaľ čo stanovenie toho, či došlo k porušeniu dôvernosti alebo integrity je pomerne jasné, stanovenie toho, či došlo k porušeniu dostupnosti už môže byť menej zrejmé. Porušenie sa bude vždy považovať za porušenie dostupnosti, ak došlo k trvalej strate alebo zničeniu osobných údajov.

Príklad

Medzi príklady straty dostupnosti patrí situácia, v ktorej boli údaje zmazané, a to buď náhodne, alebo neoprávnenou osobou, alebo v príklade bezpečne zašifrovaných údajov, došlo k strate kľúča na dešifrovanie. V prípade, že prevádzkovateľ nedokáže obnoviť prístup k údajom, napríklad zo zálohy, považuje sa to za trvalú stratu dostupnosti.

K strate dostupnosti môže dôjsť aj vtedy, keď v normálnej prevádzke organizácie dôjde k významnému narušeniu, napríklad k výpadku elektrického prúdu alebo k útoku DoS, v dôsledku čoho sú osobné údaje nedostupné.

Vzniká tu otázka, či by sa dočasná strata dostupnosti osobných údajov mala považovať za porušenie a ak áno, či je potrebné ho oznámiť. V článku 32 GDPR, „bezpečnosť spracúvania“, sa vysvetľuje, že pri vykonávaní technických a organizačných opatrení s cieľom zaistiť úroveň bezpečnosti primeranú riziku, by sa mala okrem iného zohľadniť aj „schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb“ a „schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu“.

Z toho dôvodu bezpečnostný incident, ktorý vedie k tomu, že osobné údaje sú v určitom období nedostupné, je tiež typ porušenia, keďže nedostatočný prístup k údajom môže mať významný vplyv na práva a slobody fyzických osôb. Aby bolo jasné, situácia, kedy sú osobné údaje nedostupné v dôsledku vykonávania plánovanej údržby systému, nepredstavuje „porušenie bezpečnosti“ podľa článku 4 ods. 12.

Pokiaľ ide o trvalú stratu alebo zničenie osobných údajov (alebo v skutku akékoľvek iné porušenie), porušenie, v rámci ktorého došlo k dočasnej strate dostupnosti by sa malo zdokumentovať podľa článku 33 ods. 5. To prevádzkovateľovi pomáha pri preukazovaní zodpovednosti dozornému orgánu, ktorý môže požiadať o nahliadnutie do týchto záznamov[16]. V závislosti od okolností porušenia sa však môže alebo nemusí vyžadovať oznámenie dozornému orgánu a informovanie dotknutých osôb. Prevádzkovateľ bude musieť posúdiť pravdepodobnosť a závažnosť vplyvu na práva a slobody fyzických osôb v dôsledku nedostatočnej dostupnosti osobných údajov. Podľa článku 33 prevádzkovateľ bude musieť oznámiť porušenie, s výnimkou prípadov, keď nie je pravdepodobné, že porušenie povedie k riziku pre práva a slobody jednotlivcov. Samozrejme je potrebné to vykonávať na individuálnom základe.

Príklady

Ak v kontexte nemocnice nie sú k dispozícii kritické lekárske údaje o pacientoch, hoci len dočasne, môže to predstavovať riziko pre práva a slobody jednotlivcov, napríklad môže dôjsť k zrušeniu operácií a ohrozeniu životov.

Naopak, ak niekoľko hodín nie sú k dispozícii systémy mediálnej spoločnosti (napr. v dôsledku výpadku elektrickej energie) a táto spoločnosť potom nemôže zasielať novinky svojim odberateľom, je nepravdepodobné, že to predstavuje riziko pre práva a slobody jednotlivcov.

Treba poznamenať, že hoci strata dostupnosti systémov prevádzkovateľa môže byť len dočasná a nemusí mať vplyv na jednotlivcov, je dôležité, aby prevádzkovateľ zvážil všetky možné dôsledky porušenia, keďže stále sa môže vyžadovať oznámenie porušenia z iných dôvodov.

[16] Pozri článok 33 ods. 5.

Príklad

Napadnutie prostredníctvom softvéru ransomware (škodlivý softvér, ktorý zašifruje údaje prevádzkovateľa až do zaplatenia výkupného) by mohol viesť k dočasnej strate dostupnosti, ak je možné obnoviť údaje zo zálohy. Dochádza však k narušeniu siete a ak sa incident kvalifikuje ako porušenie dôvernosti (t. j. útočník sa dostane k osobným údajom) a to predstavuje riziko pre práva a slobody jednotlivcov, mohlo by sa vyžadovať oznámenie.

3. Potenciálne dôsledky porušenia ochrany osobných údajov

Porušenie môže mať potenciálne celý rad významných negatívnych dôsledkov na jednotlivcov, čo môže mať za následok ujmu na zdraví, majetkovú alebo nemajetkovú ujmu. V GDPR sa vysvetľuje, že to môže zahŕňať stratu kontroly nad svojimi osobnými údajmi, obmedzenie práv týchto osôb, diskrimináciu, krádež totožnosti alebo podvod, finančnú stratu, neoprávnenú reverznú pseudonymizáciu, poškodenie dobrého mena, stratu dôvernosti osobných údajov chránených profesijným tajomstvom. Môže to zahŕňať aj akékoľvek iné závažné hospodárske či sociálne znevýhodnenie týchto osôb[17].

V GDPR sa preto vyžaduje, aby prevádzkovateľ oznámil porušenie príslušnému dozornému orgánu, s výnimkou prípadov, keď nie je pravdepodobné, že toto porušenie povedie k riziku vzniku takýchto nepriaznivých dôsledkov. Ak existuje pravdepodobné vysoké riziko vzniku týchto nepriaznivých dôsledkov, v GDPR sa vyžaduje, aby prevádzkovateľ oznámil porušenie dotknutým osobám čo najskôr je to možné[18].

V odôvodnení 87 GDPR sa zdôrazňuje dôležitosť schopnosti identifikovať porušenie, posúdiť riziko pre jednotlivcov a v prípade potreby oznámiť porušenie:

„Malo by sa zistiť, či sa prijali všetky primerané technické ochranné a organizačné opatrenia na bezodkladné zistenie, či došlo k porušeniu ochrany osobných údajov, a na promptné informovanie dozorného orgánu a dotknutej osoby. Malo by sa zistiť, či sa oznámenie uskutočnilo bez zbytočného odkladu, pričom sa zohľadňuje najmä povaha a závažnosť porušenia ochrany osobných údajov, dôsledky tohto porušenia a nepriaznivé dôsledky pre dotknutú osobu. Toto oznámenie môže viesť k zásahu dozorného orgánu v súlade s jeho úlohami a právomocami ustanovenými v tomto nariadení.“

Ďalšie usmernenia týkajúce sa posúdenia rizík nepriaznivých dôsledkov na jednotlivcov sú uvedené v oddiele IV.

Ak prevádzkovatelia neoznámia porušenie ochrany údajov dozornému orgánu alebo dotknutým osobám, alebo obom, aj keď sú splnené požiadavky článkov 33 a/alebo 34, dozorný orgán má možnosť voľby, v rámci ktorej musí vziať do úvahy všetky nápravné opatrenia, ktoré má k dispozícii, čo by zahŕňalo posúdenie uloženia primeranej správnej pokuty[19], buď spolu s nápravným opatrením podľa článku 58 ods. 2, alebo samostatne. Ak sa zvolí správna pokuta, jej hodnota môže byť až do výšky 10 000 000 EUR, alebo v prípade podniku až do výšky 2 % celkového svetového ročného obratu podľa článku 83 ods. 4 písm. a) GDPR. Okrem toho je dôležité mať na zreteli, že v niektorých prípadoch by neoznámenie porušenia mohlo odhaliť buď neexistenciu súčasných bezpečnostných opatrení, alebo neprimeranosť súčasných bezpečnostných opatrení. V usmerneniach pracovnej skupiny podľa článku 29 týkajúcich sa správnych pokút sa uvádza: „Pokiaľ sa v jednom konkrétnom

[17] Pozri aj odôvodnenia 85 a 75.

[18] Pozri aj odôvodnenie 86.

[19] Ďalšie podrobnosti sa nachádzajú v usmerneniach pracovnej skupiny podľa článku 29 o uplatňovaní a stanovovaní správnych pokút, ktoré sú k dispozícii na adrese: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

prípade vyskytlo viacero rôznych porušení, znamená to, že dozorný orgán môže uplatniť správne pokuty na úrovni, ktorá je účinná, primeraná a odradzujúca v medziach najzávažnejšieho porušenia". Dozorný orgán bude mať v takom prípade navyše možnosť uložiť sankcie za neoznámenie porušenia (články 33 a 34) na jednej strane a za neexistenciu (primeraných) bezpečnostných opatrení (článok 32) na strane druhej, keďže ide o dve samostatné porušenia.

II. Článok 33 – Oznámenie porušenia ochrany osobných údajov dozornému orgánu

A. Kedy podať oznámenie

1. Článok 33 požiadavky

V článku 33 ods. 1 sa uvádza:

> „V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania."

V odôvodnení 87 sa stanovuje[20]:

> „Malo by sa zistiť, či sa prijali všetky primerané technické ochranné a organizačné opatrenia na bezodkladné zistenie, či došlo k porušeniu ochrany osobných údajov, a na promptné informovanie dozorného orgánu a dotknutej osoby. Malo by sa zistiť, či sa oznámenie uskutočnilo bez zbytočného odkladu, pričom sa zohľadňuje najmä povaha a závažnosť porušenia ochrany osobných údajov, dôsledky tohto porušenia a nepriaznivé dôsledky pre dotknutú osobu. Toto oznámenie môže viesť k zásahu dozorného orgánu v súlade s jeho úlohami a právomocami ustanovenými v tomto nariadení."

2. Kedy sa o tom „dozvie" prevádzkovateľ?

Ako už bolo uvedené, v GDPR sa vyžaduje, aby v prípade porušenia prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámil toto porušenie. To môže viesť k otázke, kedy možno prevádzkovateľa považovať za „vedomého" porušenia. Pracovná skupina podľa článku 29 sa domnieva, že prevádzkovateľ by sa mal považovať za „vedomého", keď má tento prevádzkovateľ primeranú úroveň istoty, že došlo k bezpečnostnému incidentu, ktorý viedol k ohrozeniu osobných údajov.

Ako však už bolo uvedené, v GDPR sa vyžaduje, aby prevádzkovateľ prijal všetky primerané technické ochranné a organizačné opatrenia na bezodkladné zistenie, či došlo k porušeniu, a na promptné informovanie dozorného orgánu a dotknutých osôb. Uvádza sa v ňom aj to, že by sa malo zistiť, či sa oznámenie uskutočnilo bez zbytočného odkladu, pričom sa zohľadňuje najmä povaha a závažnosť porušenia, dôsledky tohto porušenia a nepriaznivé dôsledky pre dotknutú osobu[21]. Týmto sa prevádzkovateľovi ukladá povinnosť zabezpečiť, aby sa včas dozvedel o všetkých porušeniach, aby tak mohol prijať primerané opatrenia.

---

20 Tu je dôležité aj odôvodnenie 85.

21 Pozri odôvodnenie 87.

To, kedy presne možno prevádzkovateľa považovať za „vedomého“ konkrétneho porušenia, bude závisieť od okolností daného porušenia. V niektorých prípadoch bude od začiatku pomerne jasné, že došlo k porušeniu, zatiaľ čo v iných prípadoch môže trvať určitý čas, kým sa zistí, či boli osobné údaje ohrozené. Dôraz by sa však mal klásť na rýchle kroky na vyšetrenie incidentu, aby sa zistilo, či bola porušená ochrana osobných údajov a ak áno, na prijatie nápravných opatrení a v prípade potreby na oznámenie.

Príklady

1. V prípade USB kľúča s nezašifrovanými osobnými údajmi často nie je možné zistiť, či neoprávnené osoby získali prístup k týmto údajom. Napriek tomu, hoci prevádzkovateľ nemusí byť schopný zistiť, či došlo k porušeniu dôvernosti, sa takýto prípad musí oznámiť, keďže existuje primeraná úroveň istoty, že došlo k porušeniu dostupnosti; prevádzkovateľ sa o tom dozvie, keď si uvedomí, že USB kľúč sa stratil.

2. Tretia strana informuje prevádzkovateľa, že omylom získala osobné údaje jedného z jeho zákazníkov a poskytne dôkaz o neoprávnenom poskytnutí údajov. Vzhľadom na to, že prevádzkovateľovi sa predložili jasné dôkazy o porušení dôvernosti, nemožno pochybovať o tom, že si je toho „vedomý“.

3. Prevádzkovateľ zistí, že došlo k možnému narušeniu jeho siete. Prevádzkovateľ skontroluje svoje systémy s cieľom zistiť, či osobné údaje uchovávané v tomto systéme boli ohrozené a potvrdí, že k tomu došlo. Opäť, vzhľadom na to, že teraz má prevádzkovateľovi jasné dôkazy o porušení, nemožno pochybovať o tom, že si je toho „vedomý“.

4. Páchateľ počítačovej trestnej činnosti kontaktuje prevádzkovateľa po tom, ako napadne jeho systém s cieľom žiadať o výkupné. V takomto prípade má prevádzkovateľ po skontrolovaní svojho systému na účely potvrdenia, že bol napadnutý, jasné dôkazy o tom, že došlo k porušeniu a nemožno pochybovať o tom, že si je toho „vedomý“.

Prevádzkovateľ po tom, ako ho o možnom porušení prvýkrát informuje jednotlivec, mediálna organizácia alebo iný zdroj, alebo po tom, ako sám odhalí bezpečnostný incident, môže vykonať krátkodobé vyšetrovanie s cieľom zistiť, či skutočne došlo k porušeniu alebo nie. Počas tohto obdobia vyšetrovania prevádzkovateľa nemožno považovať za „vedomého“. Očakáva sa však, že počiatočné vyšetrovanie by sa malo začať čo najskôr a v rámci neho by sa malo zistiť s primeranou úrovňou istoty, či došlo k porušeniu; potom môže nasledovať podrobnejšie vyšetrovanie.

Keď sa to prevádzkovateľ dozvie, porušenie podliehajúce oznamovacej povinnosti sa musí bez zbytočného odkladu a podľa možnosti najneskôr do 72 oznámiť. Počas tohto obdobia by mal prevádzkovateľ posúdiť pravdepodobné riziko pre jednotlivcov s cieľom zistiť, či vznikol podnet na požiadavku na oznámenie, ako aj kroky potrebné na riešenie tohto porušenia. Prevádzkovateľ však už môže mať počiatočné posúdenie potenciálneho rizika, ktoré by mohlo vyplynúť z porušenia ako súčasti posúdenia vplyvu na ochranu údajov[22] vykonaného pred uskutočnením príslušnej spracovateľskej operácie. Posúdenie vplyvu na ochranu údajov však môže byť všeobecnejšie v porovnaní s konkrétnymi okolnosťami prípadného skutočného porušenia, a preto v každom prípade bude potrebné vykonať dodatočné posúdenie zohľadňujúce tieto okolnosti. Podrobnejšie informácie o posúdení rizika sa nachádzajú v oddiele IV.

Vo väčšine prípadov by sa tieto predbežné opatrenia mali vykonať krátko po počiatočnom upozornení (teda keď má prevádzkovateľ alebo sprostredkovateľ podozrenie, že došlo k bezpečnostnému incidentu, ktorý sa môže týkať osobných údajov) – dlhšie by to malo trvať iba vo výnimočných prípadoch.

[22] Pozri usmernenia pracovnej skupiny podľa článku 29 o posúdeniach vplyvu na ochranu údajov na tejto adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Príklad

Jednotlivec informuje prevádzkovateľa, že dostal email, ktorý sa javí byť od prevádzkovateľa a obsahuje osobné údaje týkajúce sa jeho (skutočného) používania služby prevádzkovateľa, pričom naznačuje, že bezpečnosť prevádzkovateľa bola ohrozená. Prevádzkovateľ vykoná krátkodobé vyšetrovanie a odhalí narušenie svojej siete a dôkazy o neoprávnenom prístupe k osobným údajom. Prevádzkovateľ sa teraz považuje za „vedomého“ a vyžaduje sa oznámenie dozornému orgánu, s výnimkou prípadu, kedy je nepravdepodobné, že by porušenie mohlo viesť k ohrozeniu práv a slobôd jednotlivcov. Prevádzkovateľ bude musieť prijať primerané nápravné opatrenia na riešenie porušenia.

Prevádzkovateľ by preto mal mať zavedené vnútorné postupy, aby dokázal odhaliť a riešiť porušenie. Napríklad na nájdenie určitých nezrovnalostí v spracúvaní údajov môže prevádzkovateľ alebo sprostredkovateľ použiť určité technické opatrenia, ako sú analyzátory toku údajov a protokolov o činnostiach, z ktorých je možné určiť udalosti a upozornenia korelovaním všetkých údajov z protokolu o činnostiach[23]. Je dôležité, aby v prípade zistenia porušenia bolo toto porušenie oznámené vyššej príslušnej úrovni riadenia, aby ho bolo možné riešiť a v prípade potreby oznámiť v súlade s článkom 33 a prípadne s článkom 34. Takéto opatrenia a mechanizmy podávania správ by mohli byť podrobne opísané v plánoch reakcie na incidenty prevádzkovateľa a/alebo v mechanizmoch riadenia. Tieto pomôžu prevádzkovateľovi účinne plánovať a stanoviť, kto má v rámci organizácie prevádzkovú zodpovednosť za riešenie porušenia a ako alebo či v prípade potreby stupňovať incident.

Prevádzkovateľ by mal mať zavedené aj dohody s prípadnými sprostredkovateľmi, ktorých tento prevádzkovateľ využíva, ktorí sú sami povinní oznámiť prevádzkovateľovi prípadné porušenie (pozri ďalej).

Zatiaľ čo je zodpovednosťou prevádzkovateľov a sprostredkovateľov, aby zaviedli vhodné opatrenia na prevenciu porušenia, reakciu na porušenie a riešenie porušenia, existujú určité praktické kroky, ktoré by sa mali prijať vo všetkých prípadoch.

- Informácie týkajúce sa všetkých udalostí súvisiacich s bezpečnosťou by mali byť adresované zodpovednej osobe, resp. osobám, ktorých úlohou je riešiť incidenty, zisťovať prítomnosť porušenia a posudzovať riziko.
- Potom by sa malo posúdiť riziko pre jednotlivcov vyplývajúce z porušenia (pravdepodobnosť žiadneho rizika, rizika alebo vysokého rizika), pričom sa informujú príslušné časti organizácie.
- Malo by sa vykonať oznámenie dozornému orgánu a prípadne by sa o porušení mali informovať dotknuté osoby, ak je to potrebné.
- Prevádzkovateľ by súčasne mal konať tak, aby zabránil šíreniu porušenia a aby sa porušenie vyriešilo.
- V priebehu vývoja okolností súvisiacich s porušením by sa mala vykonávať dokumentácia.

Malo by teda byť jasné, že prevádzkovateľ má povinnosť konať pri akomkoľvek počiatočnom upozornení a mal by zistiť, či k porušeniu skutočne došlo, alebo nie. Toto krátke obdobie umožňuje určité vyšetrovanie a prevádzkovateľ má počas neho možnosť zhromaždiť dôkazy a iné dôležité údaje. Ak však prevádzkovateľ s primeranou úrovňou istoty zistí, že k porušeniu došlo a ak sú splnené podmienky uvedené v článku 33 ods. 1, musí to bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín oznámiť dozornému orgánu[24]. Ak prevádzkovateľ nekoná včas a je jasné, že k porušeniu došlo, mohlo by sa to považovať za neoznámenie v súlade s článkom 33.

[23] Treba poznamenať, že aj údaje z protokolu o činnostiach uľahčujúce kontrolovateľnosť, ako sú uchovávanie, úpravy alebo vymazávanie údajov, sa môžu považovať za osobné údaje týkajúce sa osoby, ktorá iniciovala príslušnú spracovateľskú operáciu.

[24] Pozri nariadenie č. 1182/71, ktorým sa stanovujú pravidlá pre lehoty, dátumy a termíny, k dispozícii na adrese: http://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:31971R1182&from=SK

V článku 32 sa objasňuje, že prevádzkovateľ a sprostredkovateľ by mali prijať primerané technické a organizačné opatrenia s cieľom zaistiť primeranú úroveň bezpečnosti osobných údajov: schopnosti včas odhaliť, riešiť a oznámiť porušenie by sa mali vnímať ako zásadné prvky týchto opatrení.

3. Spoloční prevádzkovatelia

Článok 26 sa týka spoločných prevádzkovateľov a stanovuje sa v ňom, že spoloční prevádzkovatelia určia svoje príslušné zodpovednosti za dodržiavanie GDPR[25]. To zahŕňa stanovenie, ktorá strana bude zodpovedná za plnenie povinností podľa článkov 33 a 34. Pracovná skupina podľa článku 29 odporúča, aby zmluvné dojednania medzi spoločnými prevádzkovateľmi zahŕňali ustanovenia, v ktorých sa určí, ktorý prevádzkovateľ bude mať vedúcu úlohu pri dodržiavaní povinností oznamovania porušení podľa GDPR, resp. ktorý prevádzkovateľ bude za toto dodržiavanie zodpovedný.

4. Povinnosti sprostredkovateľa

Prevádzkovateľ si ponecháva všeobecnú zodpovednosť za ochranu osobných údajov, ale sprostredkovateľ má zohrávať dôležitú úlohu, ktorou je umožniť prevádzkovateľovi plniť si jeho povinnosti, a to zahŕňa oznámenie porušenia. V článku 28 ods. 3 sa konkrétne uvádza, že spracúvanie sprostredkovateľom sa riadi zmluvou alebo iným právnym aktom. V článku 28 ods. 3 písm. f) sa uvádza, že zmluva alebo iný právny akt stanovia, že sprostredkovateľ „pomáha prevádzkovateľovi zabezpečiť plnenie povinností podľa článkov 32 až 36 s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi."

V článku 33 ods. 2 sa objasňuje, že ak prevádzkovateľ využíva sprostredkovateľa a sprostredkovateľ sa dozvie o porušení ochrany osobných údajov, ktoré spracúva v prospech prevádzkovateľa, musí to „bez zbytočného odkladu" oznámiť prevádzkovateľovi. Treba poznamenať, že sprostredkovateľ, pred tým než podá oznámenie prevádzkovateľovi, nemusí najprv posúdiť pravdepodobnosť rizika vyplývajúceho z porušenia, toto posúdenie musí vykonať prevádzkovateľ po tom, čo sa dozvie o porušení. Sprostredkovateľ musí zistiť len to, či došlo k porušeniu, a potom to musí oznámiť prevádzkovateľovi. Prevádzkovateľ využíva sprostredkovateľa na dosiahnutie svojich cieľov, prevádzkovateľ by sa mal preto v zásade považovať za „vedomého", akonáhle ho sprostredkovateľ informuje o porušení. Povinnosť sprostredkovateľa oznámiť porušenie prevádzkovateľovi umožňuje prevádzkovateľovi riešiť porušenie a určiť, či je potrebné podať oznámenie dozornému orgánu v súlade s článkom 33 ods. 1 a dotknutým osobám v súlade s článkom 34 ods. 1. Prevádzkovateľ okrem toho môže chcieť vyšetrovať porušenie, keďže sprostredkovateľ nemusí byť schopný poznať všetky relevantné skutočnosti súvisiace s danou vecou, napríklad to, či prevádzkovateľ stále uchováva kópiu alebo zálohu zničených alebo stratených osobných údajov. To môže mať vplyv na to, či to prevádzkovateľ bude musieť podať oznámenie.

V GDPR sa nestanovuje výslovná lehota, v rámci ktorej musí sprostredkovateľ upozorniť prevádzkovateľa, okrem toho, že tak musí urobiť „bez zbytočného odkladu". Pracovná skupina podľa článku 29 preto odporúča, aby sprostredkovateľ okamžite informoval prevádzkovateľa, pričom ďalšie informácie o porušení mu poskytne vo viacerých etapách, keď bude mať k dispozícii ďalšie podrobnosti. To je dôležité v záujme pomoci prevádzkovateľovi splniť požiadavku oznámenia dozornému orgánu do 72 hodín.

Ako už bolo vysvetlené, v zmluve medzi prevádzkovateľom a sprostredkovateľom by sa malo určiť, ako by sa mali plniť požiadavky uvedené v článku 33 ods. 2 okrem iných ustanovení v GDPR. To môže zahŕňať požiadavky na včasné oznamovanie zo strany sprostredkovateľa, ktoré zasa podporujú povinnosti prevádzkovateľa podávať oznámenia dozornému orgánu do 72 hodín.

---

[25] Pozri aj odôvodnenie 79.

Ak sprostredkovateľ poskytuje služby viacerým prevádzkovateľom, z ktorých sú všetci ovplyvnení rovnakým incidentom, sprostredkovateľ musí oznámiť podrobnosti incidentu každému prevádzkovateľovi.

Sprostredkovateľ by mohol podať oznámenie v mene prevádzkovateľa, ak prevádzkovateľ poskytol sprostredkovateľovi riadne povolenie a ak je to súčasťou zmluvných dojednaní medzi prevádzkovateľom a sprostredkovateľom. Takéto oznámenie sa musí vykonať v súlade s článkom 33 a článkom 34. Je však dôležité poznamenať, že právnu zodpovednosť podať oznámenie má stále prevádzkovateľ.

B. Poskytovanie informácií dozornému orgánu

1. Informácie, ktoré sa majú poskytnúť

Ak prevádzkovateľ oznámi porušenie dozornému orgánu, v článku 33 ods. 3 sa uvádza, že toto oznámenie by malo obsahovať aspoň:

„a) opis povahy porušenia ochrany osobných údajov, podľa možnosti vrátane 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 GDPR sa nedefinujú kategórie dotknutých osôb alebo záznamov o osobných údajoch. Pracovná skupina podľa článku 29 však navrhuje, aby kategórie dotknutých osôb zodpovedali rôznym typom jednotlivcov, ktorých osobné údaje boli ovplyvnené porušením: v závislosti od použitých deskriptorov by mohli byť zahrnuté okrem iného deti a iné zraniteľné skupiny, ľudia so zdravotným postihnutím, zamestnanci alebo zákazníci. Kategórie záznamov o osobných údajoch by podobne mohli zodpovedať rôznym typom záznamov, ktoré môže prevádzkovateľ spracúvať, ako sú zdravotné údaje, údaje o vzdelaní, informácie o sociálnej starostlivosti, finančné údaje, čísla bankových účtov, čísla pasov atď.

V odôvodnení 85 sa jasne uvádza, že jedným z účelov oznamovania je obmedzenie ujmy jednotlivcom. Preto ak typy dotknutých osôb alebo typy osobných údajov naznačujú riziko vzniku konkrétnej škody, ku ktorej došlo v dôsledku porušenia (napr. krádež totožnosti, podvod, finančná strata, ohrozenie profesijného tajomstva), je dôležité, aby sa v oznámení uvádzali tieto kategórie. Týmto spôsobom vznikne spojenie s požiadavkou na opis pravdepodobných dôsledkov porušenia.

Ak nie sú k dispozícii presné informácie (napr. presný počet dotknutých osôb), nemalo by to byť prekážkou včasného oznámenia porušenia. V GDPR sa umožňuje vykonanie približného odhadu počtu dotknutých osôb a počtu dotknutých záznamov o osobných údajoch. Pozornosť by sa mala zamerať skôr na riešenie nepriaznivých dôsledkov porušenia a nie na poskytovanie presných údajov. Keď sa teda zistí, že došlo k porušeniu, ale jeho rozsah ešte nie je známy, bezpečným spôsobom, ako splniť oznamovacie povinnosti, je podávanie oznámení vo viacerých etapách (pozri ďalej).

V článku 33 ods. 3 sa uvádza, že prevádzkovateľ s oznámením poskytne „aspoň“ tieto informácie, takže prevádzkovateľ sa v prípade potreby môže rozhodnúť, že poskytne ďalšie podrobnosti. Rôzne typy porušení (porušenie dôvernosti, integrity alebo dostupnosti) môžu vyžadovať poskytnutie ďalších informácií s cieľom plne vysvetliť okolnosti každého prípadu.

Príklad

Prevádzkovateľ môže v rámci oznámenia dozornému orgánu považovať za užitočné pomenovať svojho sprostredkovateľa, ak je hlavnou príčinou porušenia, najmä ak to viedlo k incidentu s vplyvom na záznamy o osobných údajoch mnohých ďalších prevádzkovateľov, ktorí využívajú rovnakého sprostredkovateľa.

Dozorný orgán môže v každom prípade požiadať o ďalšie informácie v rámci vyšetrovania porušenia.

2. Oznámenie vo viacerých etapách

V závislosti od povahy porušenia môže byť potrebné ďalšie vyšetrovanie zo strany prevádzkovateľa s cieľom zistiť všetky relevantné skutočnosti súvisiace s incidentom. V článku 33 ods. 4 sa preto uvádza:

„V rozsahu, v akom nie je možné poskytnúť informácie súčasne, možno informácie poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu."

To znamená, že v GDPR sa uznáva, že prevádzkovatelia nebudú vždy mať dostatočné informácie o porušení do 72 hodín po tom, čo sa o ňom dozvedeli, keďže úplné a komplexné informácie o incidente nie sú v počiatočnom období vždy k dispozícii. Ako také umožňuje oznámenie po viacerých etapách. Je pravdepodobnejšie, že sa to bude týkať zložitejších porušení, ako sú niektoré typy incidentov v oblasti kybernetickej bezpečnosti, pri ktorých napríklad môže byť potrebné dôkladné forenzné vyšetrovanie s cieľom plne určiť povahu porušenia a rozsah, v akom boli osobné údaje ohrozené. V mnohých prípadoch teda prevádzkovateľ bude musieť vykonať ďalšie vyšetrovanie a následné kroky s dodatočnými informáciami v neskoršej fáze. To je prípustné za predpokladu, že prevádzkovateľ uvedie dôvody omeškania v súlade s článkom 33 ods. 1. Pracovná skupina podľa článku 29 odporúča, aby prevádzkovateľ pri prvom podaní oznámenia dozornému orgánu, informoval dozorný orgán o tom, že ešte nemá všetky požadované informácie a že ďalšie údaje poskytne neskôr. Dozorný orgán by mal schváliť ako a kedy by sa mali poskytnúť dodatočné informácie. To prevádzkovateľovi nebráni v tom, aby poskytol ďalšie informácie v ktorejkoľvek inej etape, ak sa dozvie o ďalších relevantných podrobnostiach o porušení, ktoré je potrebné poskytnúť dozornému orgánu.

Zmyslom požiadavky na oznamovanie je podporiť prevádzkovateľov, aby v prípade porušenia konali rýchlo, aby zabránili jeho šíreniu a ak je to možné, aby získali späť ohrozené osobné údaje, ako aj aby vyhľadali príslušné poradenstvo od dozorného orgánu. Podanie oznámenia dozornému orgánu počas prvých 72 hodín môže prevádzkovateľovi umožniť, aby sa uistil, že rozhodnutia o informovaní alebo neinformovaní jednotlivcov sú správne.

Účelom podania oznámenia dozornému orgánu však nie je len získať usmernenie o tom, či je potrebné informovať dotknuté osoby. V niektorých prípadoch bude zrejmé, že v dôsledku povahy porušenia a závažnosti rizika bude prevádzkovateľ musieť bezodkladne informovať dotknuté osoby. Napríklad, ak existuje bezprostredná hrozba krádeže totožnosti alebo sa na internete poskytnú osobitné kategórie osobných údajov[26], prevádzkovateľ by mal bez zbytočného odkladu konať s cieľom zabrániť šíreniu porušenia a oznámiť ho dotknutým osobám (pozri oddiel III). Vo výnimočných okolnostiach sa to môže uskutočniť dokonca aj pred podaním oznámenia dozornému orgánu. Všeobecnejšie povedané, oznámenie dozornému orgánu nesmie slúžiť ako odôvodnenie neoznámenia porušenia dotknutej osobe, v prípade kedy sa vyžaduje.

Malo by byť jasné aj to, že po uskutočnení počiatočného oznámenia by prevádzkovateľ mohol poskytnúť dozornému orgánu najnovšie informácie, ak sa v ďalšom vyšetrovaní odhalia dôkazy, že bezpečnostnému incidentu sa podarilo zabrániť a nedošlo k žiadnemu porušeniu. Tieto informácie by sa potom mohli doplniť

[26] Pozri článok 9.

k informáciám, ktoré už boli poskytnuté dozornému orgánu a incident sa teda zaznamená ako neporušenie. Za nahlásenie incidentu, o ktorom sa napokon preukáže, že nie je porušením, neexistuje žiadna sankcia.

Príklad

Prevádzkovateľ do 72 hodín od zistenia porušenia oznámi dozornému orgánu, že stratil USB kľúč obsahujúci kópiu osobných údajov niektorých jeho zákazníkov. USB kľúč sa neskôr nájde na inom mieste v priestoroch prevádzkovateľa. Prevádzkovateľ poskytne dozornému orgánu najnovšie informácie a požiada o zmenu oznámenia.

Treba poznamenať, že prístup po viacerých etapách k oznámeniu sa už vzťahuje na existujúce povinnosti podľa smernice 2002/58/ES, nariadenia 611/2013 a iných subjektívne nahlásených incidentov.

3. Oneskorené oznámenia

V článku 3 ods. 1 sa objasňuje, že ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania. Toto spolu s koncepciou oznámenia po viacerých etapách vyjadruje, že prevádzkovateľ nemusí byť vždy schopný oznámiť porušenie v rámci danej lehoty a že možno pripustiť oneskorené oznámenie.

Takýto scenár by mohol nastať, ak sa napríklad prevádzkovateľ stretne s viacerými podobnými porušeniami dôvernosti v krátkom časovom období, s rovnakým vplyvom na veľký počet dotknutých osôb. Prevádzkovateľ by sa mohol dozvedieť o porušení a pri začatí vyšetrovania a pred oznámením zistiť ďalšie podobné porušenia, ktoré majú rôzne príčiny. V závislosti od okolností môže prevádzkovateľovi trvať určitý čas, kým zistí rozsah porušení a namiesto toho, aby samostatne oznamoval každé porušenie, prevádzkovateľ pripraví zmysluplné oznámenie, ktoré predstavuje niekoľko veľmi podobných porušení s možnými rôznymi príčinami. To by mohlo viesť k oneskoreniu oznámenia dozornému orgánu o viac ako 72 hodín po tom, ako sa prevádzkovateľ prvýkrát dozvedel o týchto porušeniach.

Presnejšie povedané, každé jedno porušenie je incidentom, ktorý podlieha oznámeniu. Aby sa však predišlo nadmernému zaťaženiu, prevádzkovateľ môže predložiť „zoskupené“ oznámenie predstavujúce všetky tieto porušenia, a to za predpokladu, že sa týkajú porušenia rovnakého typu ochrany osobných údajov v pomerne krátkom časovom období. Ak dôjde k viacerým porušeniam, ktoré sa týkajú rôznych typov ochrany osobných údajov, porušených rôznymi spôsobmi, podávanie oznámení by malo prebiehať obvyklým spôsobom, pričom každé porušenie sa oznamuje v súlade s článkom 33.

Zatiaľ čo sa v GDPR do istej miery umožňujú oneskorené oznámenia, nemalo by sa to vnímať ako niečo, k čomu dochádza pravidelne. Treba poznamenať, že zoskupené oznámenia možno vykonať aj v prípade viacerých podobných porušení nahlásených do 72 hodín.

C. Cezhraničné porušenia a porušenia v prevádzkarňach mimo EÚ.

1. Cezhraničné porušenia

Ak dochádza k cezhraničnému spracúvaniu[27] osobných údajov, porušenie môže mať vplyv na dotknuté osoby vo viac ako jednom členskom štáte. V článku 33 ods. 1 sa uvádza, že v prípade porušenia by mal prevádzkovateľ oznámiť túto skutočnosť dozornému orgánu príslušnému podľa článku 55 GDPR[28]. V článku 55 ods. 1 sa uvádza:

„Každý dozorný orgán je príslušný plniť úlohy, ktoré mu boli uložené, a vykonávať právomoci, ktoré mu boli zverené, v súlade s týmto nariadením na území vlastného členského štátu.“

[27] Pozri článok 4 ods. 23.

[28] Pozri aj odôvodnenie 122.

V článku 56 ods. 1 sa však uvádza:

„Bez toho, aby bol dotknutý článok 55, dozorný orgán hlavnej prevádzkarne alebo jedinej prevádzkarne prevádzkovateľa alebo sprostredkovateľa je príslušný konať ako vedúci dozorný orgán pre cezhraničné spracúvanie vykonávané zo strany tohto prevádzkovateľa alebo sprostredkovateľa v súlade s postupom stanoveným v článku 60.“

V článku 56 ods. 6 sa okrem toho uvádza:

„Vedúci dozorný orgán je jediným partnerom prevádzkovateľa alebo sprostredkovateľa v súvislosti s cezhraničným spracúvaním vykonávaným týmto prevádzkovateľom alebo sprostredkovateľom.“

To znamená, že ak dôjde k porušeniu v kontexte cezhraničného spracúvania a vyžaduje sa oznámenie, prevádzkovateľ bude musieť podať oznámenie vedúcemu dozornému orgánu[29]. Preto pri vypracovávaní plánu reakcie na porušenie musí prevádzkovateľ posúdiť, ktorý dozorný orgán je vedúcim dozorným orgánom, ktorému podá oznámenie[30]. To umožní prevádzkovateľovi ihneď reagovať na porušenie a splniť si svoje povinnosti podľa článku 33. Malo by byť jasné, že v prípade porušenia súvisiaceho s cezhraničným spracúvaním sa musí podať oznámenie vedúcemu dozornému orgánu, ktorý sa nemusí nevyhnutne nachádzať tam, kde príslušné dotknuté osoby alebo tam, kde došlo k porušeniu. Pri podávaní oznámenia vedúcemu orgánu by mal prevádzkovateľ v prípade potreby uviesť, či sa porušenie týka prevádzkarní nachádzajúcich sa v iných členských štátoch, ako aj v ktorých členských štátoch boli dotknuté osoby pravdepodobne ovplyvnené porušením. Ak má prevádzkovateľ akékoľvek pochybnosti o totožnosti vedúceho dozorného orgánu, mal by prinajmenšom podať oznámenie miestnemu dozornému orgánu na mieste, kde došlo k porušeniu.

2. Porušenia v zriadeniach mimo EÚ

Článok 3 sa týka územnej pôsobnosti GDPR, a to aj ak sa vzťahuje na spracúvanie osobných údajov prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v EÚ. V článku 3 ods. 2 sa uvádza najmä[31]:

„Toto nariadenie sa vzťahuje na spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Únii, prevádzkovateľom alebo sprostredkovateľom, ktorý nie je usadený v Únii, pričom spracovateľská činnosť súvisí:

a) s ponukou tovaru alebo služieb týmto dotknutým osobám v Únii bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba, alebo,

b) so sledovaním ich správania, pokiaľ ide o ich správanie na území Únie.“

Článok 3 ods. 3 je takisto relevantný a stanovuje sa v ňom[32]:

---

29 Pozri usmernenia pracovnej skupiny podľa článku 29 týkajúce sa identifikácie vedúceho dozorného orgánu prevádzkovateľa alebo sprostredkovateľa, ktoré sú k dispozícii na adrese http://ec.europa.eu/newsroom/document.cfm?doc_id=44102http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

30 Zoznam kontaktných údajov všetkých európskych vnútroštátnych orgánov na ochranu údajov sa nachádza na adrese: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

31 Pozri aj odôvodnenia 23 a 24.

32 Pozri aj odôvodnenie 25.

„Toto nariadenie sa vzťahuje na spracúvanie osobných údajov prevádzkovateľom, ktorý nie je usadený v Únii, ale na mieste, kde sa na základe medzinárodného práva verejného uplatňuje právo členského štátu.“

Ak sa teda na prevádzkovateľa, ktorý nie je usadený v EÚ, vzťahuje článok 3 ods. 2 alebo článok 3 ods. 3 a tento prevádzkovateľ sa stretne s porušením, stále sa na neho vzťahuje oznamovacia povinnosť podľa článku 33 a 34. V článku 27 sa vyžaduje, aby prevádzkovateľ (a sprostredkovateľ) určil zástupcu v EÚ, ak sa uplatňuje článok 3 ods. 2. V takýchto prípadoch pracovná skupina podľa článku 29 odporúča, aby sa oznámenie podalo dozornému orgánu v členskom štáte, v ktorom je usadený zástupca prevádzkovateľa v EÚ[33]. Podobne ak sa na sprostredkovateľa vzťahuje článok 3 ods. 2, budú sa na neho vzťahovať povinnosti sprostredkovateľa, najmä povinnosť oznámiť prevádzkovateľovi porušenie podľa článku 33 ods. 2.

D. Podmienky, za ktorých sa nevyžaduje oznámenie

V článku 33 ods. 1 sa objasňuje, že porušenie, v prípade ktorého „nie je pravdepodobné, že povedie k riziku pre práva a slobody fyzických osôb“, nevyžaduje oznámenie dozornému orgánu. Príkladom môže byť situácia, kedy sú osobné údaje už verejne dostupné a poskytnutie takýchto údajov nepredstavuje pravdepodobné riziko pre jednotlivca. Toto je v rozpore so súčasnými požiadavkami na oznamovanie porušenia pre poskytovateľov verejne dostupných elektronických komunikačných služieb v smernici 2009/136/ES, kde sa uvádza, že všetky príslušné porušenia sa musia oznámiť príslušnému orgánu.

Pracovná skupina podľa článku 29 vo svojom stanovisku 03/2014 k oznámeniu porušenia[34] vysvetlila, že porušenie dôvernosti osobných údajov, ktoré boli zašifrované pomocou najmodernejšieho algoritmu sa vždy považuje za porušenie ochrany osobných údajov a musí sa oznámiť. Ak je však dôvernosť kľúča neporušená – teda kľúč nebol ohrozený v prípade akéhokoľvek porušenia bezpečnosti a bol vygenerovaný tak, že osoba, ktorá nemá oprávnenie na prístup k nemu, ho nedokáže určiť pomocou dostupných technických prostriedkov – údaje sú v zásade nečitateľné. Je teda nepravdepodobné, že porušenie nepriaznivo ovplyvní jednotlivcov, a preto by nebolo potrebné informovať týchto jednotlivcov[35]. Avšak aj keď sú údaje zašifrované, strata alebo zmena môžu mať negatívne dôsledky pre dotknuté osoby v prípade, že prevádzkovateľ nemá dostatočné zálohy. V takomto prípade by sa vyžadovalo oznámenie dotknutým osobám, a to aj napriek tomu, že na samotné údaje sa vzťahovali primerané šifrovacie opatrenia.

Pracovná skupina podľa článku 29 okrem toho vysvetlila, že by to tak bolo aj v prípade, keby osobné údaje, napríklad heslá, boli bezpečne hašované a solené, hašovacia hodnota by sa vypočítala pomocou najnovšej kryptografickej šifrovanej hašovacej funkcie, kľúč použitý na hašovanie nebol ohrozený pri žiadnom porušení a kľúč použitý na hašovanie bol vygenerovaný tak, že osoba, ktorá nemá oprávnenie na prístup k nemu, ho nedokáže určiť pomocou dostupných technických prostriedkov.

Takže ak sú osobné údaje v zásade nečitateľné pre neoprávnené strany a ak sú údaje kópiou alebo existuje záloha, porušenie dôvernosti týkajúce sa riadne zašifrovaných osobných údajov sa nemusí oznamovať dozornému úradu. Je to preto, lebo nie je pravdepodobné, že takéto porušenie predstavuje riziko pre práva a slobody jednotlivcov. To samozrejme znamená, že ani jednotlivec by nemusel byť informovaný, keďže neexistuje žiadne vysoké riziko. Treba však mať na pamäti, že hoci sa oznámenie nemusí spočiatku vyžadovať, ak neexistuje pravdepodobné riziko pre práva a slobody jednotlivcov,

33 Pozri odôvodnenie 80 a článok 27.

34 Pracovná skupina podľa článku 29, stanovisko 03/2014 k oznámeniu porušenia, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

35 Pozri aj článok 4 ods. 1 a článok 2 nariadenia č. 611/2013.

v priebehu času sa to môže zmeniť a riziko by sa muselo prehodnotiť. Ak sa napríklad neskôr zistí, že kľúč je ohrozený alebo sa odhalí zraniteľnosť šifrovacieho softvéru, oznámenie sa môže vyžadovať.

Okrem toho je potrebné poznamenať, že ak dôjde k porušeniu a neexistujú žiadne zálohy šifrovaných osobných údajov, potom dôjde k porušeniu dostupnosti, čo by predstavovať riziko pre jednotlivcov, a preto sa môže vyžadovať oznámenie. Podobne ak dôjde k porušeniu, pri ktorom ide o stratu zašifrovaných údajov, aj keď existuje záloha osobných údajov, stále môže ísť o porušenie, ktoré podlieha oznámeniu, v závislosti od dĺžky času potrebného na obnovenie údajov z tejto zálohy a od vplyvu, aký má táto nedostatočná dostupnosť na jednotlivcov. V článku 32 ods. 1 písm. c) sa uvádza, že dôležitým faktorom bezpečnosti je „schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu“.

Príklad

Porušením, ktoré by nevyžadovalo oznamovanie dozornému orgánu, by bola strata bezpečne zašifrovaného mobilného zariadenia používaného prevádzkovateľom a jeho zamestnancami. Za predpokladu, že šifrovací kľúč zostane v bezpečnom vlastníctve prevádzkovateľa a nejde o jedinú kópiu osobných údajov, osobné údaje by boli pre útočníka neprístupné. To znamená, že nie je pravdepodobné, že porušenie povedie k riziku pre práva a slobody príslušných dotknutých osôb. Ak sa neskôr ukáže, že šifrovací kľúč bol ohrozený alebo že šifrovací softvér alebo algoritmus je zraniteľný, riziko pre práva a slobody fyzických osôb sa zmení, a preto sa potom môže vyžadovať oznámenie.

Ak však prevádzkovateľ nepodá oznámenie dozornému orgánu v situácii, kedy údaje skutočne neboli bezpečne zašifrované, ide o nedodržanie článku 33. Preto by pri výbere šifrovacieho softvéru prevádzkovatelia mali dôkladne zvážiť kvalitu a správne vykonanie ponúkaného šifrovania, mali by chápať, akú úroveň ochrany skutočne poskytuje a či je to vhodné vzhľadom na uvedené riziká. Prevádzkovatelia by si mali byť vedomí aj špecifík fungovania ich šifrovacieho produktu. Napríklad zariadenie sa môže zašifrovať po vypnutí, ale nie v pohotovostnom režime. Niektoré produkty používajúce šifrovanie majú „predvolené kľúče“, ktoré musí každý zákazník zmeniť, ak majú byť účinné. Šifrovanie okrem toho môžu odborníci v oblasti bezpečnosti v súčasnosti považovať za primerané, ale o niekoľko rokov môže byť zastarané, čo znamená, že je otázne, či by boli údaje dostatočne šifrované takýmto produktom a či by sa poskytovala primeraná úroveň ochrany.

III. Článok 34 – Oznámenie dotknutej osobe

A. Informovanie jednotlivcov

V určitých prípadoch sa okrem oznamovania dozornému orgánu vyžaduje, aby prevádzkovateľ oznámil porušenie aj dotknutým osobám.

V článku 34 ods. 1 sa uvádza:

„V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.“

Prevádzkovatelia by mali mať na pamäti, že oznámenie dozornému orgánu je povinné, s výnimkou prípadov, kedy je nepravdepodobné, že by porušenie mohlo viesť k ohrozeniu práv a slobôd jednotlivcov. Navyše, ak je vysoko pravdepodobné, že by porušenie mohlo viesť k ohrozeniu práv a slobôd jednotlivcov, jednotlivci musia byť tiež informovaní. Prahová hodnota pre oznamovanie porušenia jednotlivcom je teda vyššia ako pri oznamovaní dozornému orgánu, a preto sa nebude vyžadovať, aby sa všetky porušenia oznamovali jednotlivcom, čo ich ochráni pred zbytočnou tzv. notifikačnou únavou.

V GDPR sa uvádza, že oznámenie porušenia jednotlivcom by sa malo vykonať „bez zbytočného odkladu“, teda čo najskôr. Hlavným cieľom oznámenia jednotlivcom je poskytnúť konkrétne informácie o krokoch, ktoré by mali podniknúť, aby sa ochránili[36]. Ako už bolo uvedené, v závislosti od povahy porušenia a možného rizika, včasné oznámenie pomôže jednotlivcom podniknúť kroky na vlastnú ochranu pred akýmikoľvek negatívnymi dôsledkami porušenia.

V prílohe B k týmto usmerneniam sa nachádza neúplný zoznam príkladov situácií, kedy je pravdepodobné, že porušenie môže viesť k vysokému riziku pre jednotlivcov, a teda aj situácií, kedy musí prevádzkovateľ informovať dotknuté osoby o porušení.

B. Informácie, ktoré sa majú poskytnúť

Pokiaľ ide o oznamovanie jednotlivcom, v článku 34 ods. 2 sa stanovuje, že:

> „Oznámenie dotknutej osobe uvedené v odseku 1 tohto článku obsahuje jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň informácie a opatrenia uvedené v článku 33 ods. 3 písm. b), c) a d)“.

Podľa tohto ustanovenia by mal prevádzkovateľ poskytnúť aspoň tieto informácie:

- opis právnej povahy porušenia,
- meno a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta,
- opis pravdepodobných dôsledkov porušenia, ako aj
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom riešiť porušenie, prípadne vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Ako príklad opatrení prijatých na riešenie porušenia a na zmiernenie jeho možných nepriaznivých dôsledkov by prevádzkovateľ mohol uviesť, že po oznámení porušenia príslušnému dozornému orgánu, prevádzkovateľ získal poradenstvo v súvislosti so spravovaním porušenia a so zmiernením jeho vplyvu. Prevádzkovateľ by mal v prípade potreby poskytnúť aj konkrétne rady jednotlivcom, aby sa chránili pred možnými nepriaznivými dôsledkami porušenia, napríklad obnovením hesiel v prípade, že ich prístupové údaje boli ohrozené. Prevádzkovateľ sa opäť môže rozhodnúť, či poskytne informácie nad rámec toho, čo sa vyžaduje.

C. Kontaktovanie jednotlivcov

Príslušné porušenie by sa v zásade malo oznámiť predmetným dotknutým osobám priamo, pokiaľ by takýto krok nepredstavoval 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 [článok 34 ods. 3 písm. c)].

Pri oznamovaní porušenia dotknutým osobám by sa mali používať špecializované správy a nemali by sa zasielať s inými informáciami, ako sú pravidelné aktualizácie, novinky alebo štandardné správy. To napomáha tomu, aby bolo oznámenie o porušení jasné a transparentné.

Príklady transparentných komunikačných metód zahŕňajú priamy prenos správ (napr. email, SMS, priama správa), nápadné bannery alebo oznámenia na webovom sídle, poštovú komunikáciu a nápadné reklamy v tlačových médiách. Oznámenie obmedzujúce sa len na tlačovú správu alebo na firemný blog by nebolo účinným prostriedkom na oznamovanie porušenia jednotlivcovi. Pracovná skupina podľa článku 29 odporúča, aby si prevádzkovatelia vybrali prostriedky, ktoré maximalizujú možnosť riadneho informovania všetkých dotknutých osôb. V závislosti od okolností to môže

[36] Pozri aj odôvodnenie 86.

znamenať, že prevádzkovateľ využíva niekoľko spôsobov komunikácie na rozdiel od používania jedného kontaktného kanála.

Prevádzkovatelia okrem toho môžu potrebovať zabezpečiť, aby bolo oznámenie dostupné v primeraných alternatívnych formátoch a príslušných jazykoch, aby sa uistili, že jednotlivci sú schopní pochopiť informácie, ktoré sú im poskytované. Napríklad pri oznamovaní porušenia jednotlivcovi bude obvykle vhodným jazykom ten, ktorý sa používal počas predchádzajúcej bežnej podnikateľskej činnosti s príjemcom. Ak má však porušenie vplyv na dotknuté osoby, s ktorými prevádzkovateľ v minulosti nekomunikoval, alebo najmä na tie osoby, ktoré majú pobyt v inom členskom štáte alebo v krajine mimo EÚ inej, než je tá, v ktorej je usadený prevádzkovateľ, mala by byť prijateľná komunikácia v miestnom štátnom jazyku s prihliadnutím na požadované zdroje. Základom je pomôcť dotknutým osobám pochopiť povahu porušenia a kroky, ktoré môžu podniknúť, aby sa chránili.

Prevádzkovatelia sú v najlepšej pozícii na to, aby určili najvhodnejší kontaktný kanál na oznámenie porušenia jednotlivcom, najmä ak so svojimi zákazníkmi komunikujú pravidelne. Je však zjavné, že prevádzkovateľ by mal byť opatrný pri používaní kontaktného kanála ohrozeného porušením, keďže tento kanál by mohol byť použitý aj útočníkmi, ktorí vystupujú ako prevádzkovateľ.

V odôvodnení 86 sa súčasne vysvetľuje, že:

> „Takéto informovanie dotknutých osôb by sa malo vykonať čo najskôr je to možné, a v úzkej spolupráci s dozorným orgánom v súlade s usmerneniami tohto alebo iného relevantného orgánu, napríklad orgánov presadzovania práva. Napríklad potreba zmierniť bezprostredné riziko škody by si vyžadovala promptné informovanie dotknutých osôb, avšak potreba vykonať primerané opatrenia na zabránenie trvaniu alebo výskytu podobných porušení ochrany osobných údajov môže opodstatniť aj dlhšiu lehotu na informovanie.“

Prevádzkovatelia by sa preto mali obrátiť na dozorný orgán nielen s cieľom získať poradenstvo o informovaní dotknutých osôb o porušení v súlade s článkom 34, ale aj v súvislosti s primeranými správami, ktoré sa majú posielať jednotlivcom, a s najvhodnejším spôsobom kontaktovania jednotlivcov.

S týmto súvisí odporúčanie v odôvodnení 88, že pri oznámení porušenia by sa mali zohľadňovať aj oprávnené záujmy orgánov presadzovania práva v prípadoch, v ktorých by predčasné poskytnutie informácií mohlo zbytočne brániť vyšetrovaniu okolností porušenia ochrany osobných údajov“. To môže znamenať, že za určitých okolností, pokiaľ je to opodstatnené, a na základe odporúčania orgánov presadzovania práva, môže prevádzkovateľ odložiť oznámenie porušenia dotknutým osobám dovtedy, kým tým nebude dotknuté takéto vyšetrovanie. Po uplynutí tohto času je však stále potrebné informovať dotknuté osoby.

Ak prevádzkovateľ nedokáže jednotlivcovi oznámiť porušenie, pretože nemá k dispozícii dostatočné údaje na to, aby kontaktoval jednotlivca, v takejto konkrétnej situácii by mal prevádzkovateľ informovať jednotlivca hneď, ako je to možné (napr. keď si jednotlivec uplatňuje svoje právo na prístup k osobným údajom podľa článku 15 a poskytne prevádzkovateľovi potrebné dodatočné kontaktné informácie).

D. Podmienky, za ktorých sa nevyžaduje oznámenie

V článku 34 ods. 3 sa uvádzajú tri podmienky, ktoré ak sú splnené, oznámenie jednotlivcom v prípade porušenia sa nevyžaduje. Ide o tieto podmienky:

- prevádzkovateľ prijal primerané technické a organizačné opatrenia na ochranu osobných údajov pred porušením, najmä tie opatrenia, ktorými sa zabezpečuje, že osobné údaje sú

nečitateľné všetkým osobám bez oprávneného prístupu k týmto údajom. To by mohlo zahŕňať napríklad ochranu osobných údajov pomocou najmodernejšieho šifrovania alebo tokenizácie,

- bezprostredne po porušení prevádzkovateľ prijal opatrenia, aby zabezpečil, že vysoké riziko pre práva a slobody jednotlivcov pravdepodobne už nebude mať dôsledky. Napríklad, v závislosti od okolností prípadu, mohol prevádzkovateľ okamžite identifikovať jednotlivca a podniknúť kroky proti tomuto jednotlivcovi, ktorý pristúpil k údajom skôr, než s nimi mohol niečo urobiť. Stále je potrebné venovať náležitú pozornosť možným dôsledkom každého porušenia dôvernosti, a to opäť v závislosti od povahy príslušných údajov,
- kontaktovať jednotlivcov by vyžadovalo neprimerané úsilie[37], napríklad ak sa ich kontaktné údaje stratili v dôsledku porušenia alebo v prvom rade nie sú známe. Napríklad, došlo k vytopeniu skladu štatistického úradu a dokumenty obsahujúce osobné údaje boli uchovávané len v papierovej forme. Prevádzkovateľ musí namiesto toho vykonať verejné oznámenie alebo prijať podobné opatrenie, čím sa zaručí, že jednotlivci budú informovaní rovnako účinným spôsobom. V prípade neprimeraného úsilia by sa mohlo uvažovať aj o technických opatreniach, aby boli informácie o porušení k dispozícii na požiadanie, čo by mohlo byť užitočné pre tých jednotlivcov. ktorí môžu byť dotknutí porušením, ale prevádzkovateľ ich nedokáže inak kontaktovať.

V súlade so zásadou zodpovednosti by prevádzkovatelia mali byť schopní preukázať dozornému orgánu, že spĺňajú jednu alebo viac z týchto podmienok[38]. Treba mať na pamäti, že hoci sa oznámenie nemusí spočiatku vyžadovať, ak neexistuje riziko pre práva a slobody fyzických osôb, v priebehu času sa to môže zmeniť a riziko by sa muselo prehodnotiť.

Ak sa prevádzkovateľ rozhodne neoznámiť porušenie jednotlivcovi, v článku 34 ods. 4 sa vysvetľuje, že dozorný orgán môže po zvážení pravdepodobnosti porušenia vedúceho k vysokému riziku požadovať, aby tak urobil. Prípadne môže dospieť k záveru, že boli splnené podmienky podľa článku 34 ods. 3, pričom v takom prípade sa nevyžaduje oznámenie jednotlivcom. Ak dozorný orgán určí, že rozhodnutie o neoznámení dotknutým osobám nie je dostatočne opodstatnené, môže zvážiť použitie svojich právomocí a sankcií, ktoré má k dispozícii.

IV. **Posúdenie rizika a vysokého rizika**

A. Riziko ako podnet pre oznámenie

Hoci sa v GDPR zavádza povinnosť oznámiť porušenie, nie je to za každých okolností podmienkou:

- oznámenie príslušnému dozornému orgánu sa vyžaduje s výnimkou prípadov, kedy je nepravdepodobné, že by porušenie mohlo viesť k ohrozeniu práv a slobôd jednotlivcov.
- podnet na oznámenie porušenia jednotlivcovi vzniká, len ak je pravdepodobné, že porušenie povedie k vysokému riziku pre jeho práva a slobody.

To znamená, že hneď, ako sa prevádzkovateľ dozvie o porušení, je mimoriadne dôležité, aby sa nielenže usiloval o zabránenie šíreniu porušenia, ale aby súčasne posúdil riziko, ku ktorému by mohlo viesť. Má to dva dôležité dôvody: po prvé, vedomosť o pravdepodobnosti a potenciálnej závažnosti vplyvu na jednotlivca pomôže prevádzkovateľovi prijať účinné opatrenia na zabránenie šíreniu a riešenie porušenia, po druhé, pomôže to prevádzkovateľovi určiť, či sa vyžaduje oznámenie dozornému orgánu a ak áno, či sa vyžaduje oznámenie dotknutým osobám.

---

[37] Pozri usmernenia pracovnej skupiny podľa článku 29 o transparentnosti, v ktorých sa zvažuje otázka neprimeraného úsilia, k dispozícii na adrese http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Pozri článok 5 ods. 2.

Ako už bolo vysvetlené, oznámenie porušenia sa vyžaduje, s výnimkou prípadov, kedy je nepravdepodobné, že by mohlo viesť k riziku pre práva a slobody jednotlivcov, a hlavným podnetom, ktorý si vyžaduje oznámenie porušenia dotknutým osobám, je situácia, kedy je pravdepodobné, že by mohlo viesť k vysokému riziku pre práva a slobody jednotlivcov. Toto riziko existuje, ak porušenie môže viesť k ujme na zdraví, majetkovej alebo nemajetkovej ujme osôb, ktorých ochrana údajov bola porušená. Príkladmi takejto ujmy sú diskriminácia, krádež totožnosti alebo podvod, finančná strata, poškodenie dobrého mena. Ak sa porušenie týka osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenia alebo členstvo v odboroch, alebo zahŕňajú genetické údaje, údaje týkajúce sa zdravia alebo údaje o sexuálnom živote, alebo údaje týkajúce sa uznania viny za trestné činy a priestupky alebo súvisiacich bezpečnostných opatrení, je pravdepodobné, že k takejto ujme dôjde[39].

B. Faktory, ktoré treba vziať do úvahy pri posudzovaní rizika

V odôvodneniach 75 a 76 GDPR sa naznačuje, že pri posudzovaní rizika je vo všeobecnosti potrebné zvážiť pravdepodobnosť a závažnosť rizika pre práva a slobody dotknutých osôb. Ďalej sa tu uvádza, že riziko by sa malo hodnotiť na základe objektívneho posúdenia.

Treba poznamenať, že posúdenie rizika pre práva a slobody osôb, ktoré je dôsledkom porušenia, má iné zameranie ako riziko posudzované v posúdení vplyvu na ochranu údajov[40]. V posúdení vplyvu na ochranu údajov sa posudzujú riziká spracúvania údajov vykonávaného podľa plánu, ako aj riziká v prípade porušenia. Pri posudzovaní možného porušenia sa v ňom všeobecne rieši pravdepodobnosť vzniku porušenia a ujma dotknutej osobe, ku ktorej by viedlo, inými slovami ide o posúdenie hypotetickej udalosti. Pri skutočnom porušení sa už udalosť vyskytla, a preto sa pozornosť venuje výlučne výslednému riziku vplyvu porušenia na jednotlivcov.

Príklad

V posúdení vplyvu na ochranu údajov sa naznačuje, aby navrhované použitie konkrétneho bezpečnostného softvérového produktu na ochranu osobných údajov bolo vhodným opatrením na zabezpečenie úrovne bezpečnosti zodpovedajúcej riziku, ktoré by inak spracúvanie predstavovalo pre jednotlivcov. Ak sa však zraniteľnosť neskôr stane známou, zmení sa tým vhodnosť softvéru na zabránenie šíreniu rizika pre chránené osobné údaje, a preto by bolo potrebné opätovné posúdenie v rámci prebiehajúceho posúdenia vplyvu na ochranu údajov.

Zraniteľnosť produktu sa neskôr zneužije a dôjde k porušeniu. Prevádzkovateľ by mal posúdiť konkrétne okolnosti porušenia, dotknuté údaje a možnú úroveň vplyvu na jednotlivcov, ako aj pravdepodobnosť, že toto riziko bude mať dôsledky.

Takže pri posudzovaní rizika pre jednotlivcov, ktoré je dôsledkom porušenia, prevádzkovateľ musí zvážiť konkrétne okolnosti porušenia vrátane závažnosti možného vplyvu a pravdepodobnosti, že k nemu dôjde. Pracovná skupina podľa článku 29 preto odporúča, aby sa v posúdení zohľadnili tieto kritériá[41]:

- Typ porušenia

39 Pozri odôvodnenie 75 a odôvodnenie 85.

40 Pozri usmernenia pracovnej skupiny o posúdeniach vplyvu na ochranu údajov na tejto adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

41 V článku 3 ods. 2 nariadenia č. 611/2013 sa uvádza usmernenie týkajúce sa faktorov, ktoré by sa mali vziať do úvahy v súvislosti s oznámením porušení v sektore elektronických komunikačných služieb, čo môže byť užitočné v kontexte oznámení podľa GDPR. Pozri http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:sk:PDF.

Typ porušenia, ku ktorému došlo, môže mať vplyv na úroveň rizika, ktoré hrozí jednotlivcom. Napríklad porušenie dôvernosti, pri ktorom sa lekárske informácie poskytli neoprávneným stranám, môže mať pre jednotlivca odlišné dôsledky v porovnaní s porušením, kedy sa lekárske informácie jednotlivca stratili alebo už nie sú k dispozícii.

- Povaha, citlivosť a objem osobných údajov

Kľúčovým faktorom pri posudzovaní rizika je samozrejme typ a citlivosť osobných údajov, ktoré boli ohrozené porušením. Obvykle platí, že čím sú údaje citlivejšie, tým je vyššie riziko ujmy pre dotknuté osoby, ale do úvahy by sa mali vziať aj iné osobné údaje o dotknutej osobe, ktoré už môžu byť k dispozícii. Napríklad je nepravdepodobné, aby poskytnutie mena a adresy osoby za bežných okolností spôsobilo značnú ujmu. Ak sa však meno a adresa adoptívneho rodiča poskytnú biologickému rodičovi, dôsledky by mohli byť veľmi závažné ako pre adoptívneho rodiča, tak aj pre dieťa.

Porušenia zahŕňajúce údaje o zdravotnom stave, doklady totožnosti alebo finančné údaje, ako sú údaje o kreditnej karte, môžu sami osebe spôsobiť ujmu, ak sa však použijú spolu, môžu sa použiť na krádež identity. Kombinácia osobných údajov je obvykle citlivejšia ako jedna časť osobných údajov.

Niektoré typy osobných údajov sa môžu na prvý pohľad zdať pomerne neškodné, malo by sa však starostlivo zvážiť, čo tieto údaje môžu odhaliť o dotknutej osobe. Zoznam zákazníkov, ktorí prijímajú pravidelné dodávky, nemusí byť obzvlášť citlivý, ale rovnaké údaje o zákazníkoch, ktorí požiadali o zastavenie ich dodávok počas dovolenky, by boli užitočnými informáciami pre zločincov.

Podobne malé množstvo veľmi citlivých osobných údajov môže mať veľký vplyv na jednotlivca a veľké množstvo údajov môže odhaliť väčší rozsah informácií o tejto osobe. Navyše narušenie, ktoré má vplyv na veľké objemy osobných údajov o mnohých dotknutých osobách, môže mať vplyv na zodpovedajúci veľký počet osôb.

- Jednoduchosť identifikácie jednotlivcov

Dôležitým faktorom, ktorý je potrebné vziať do úvahy, je aké jednoduché bude pre stranu, ktorá má prístup k ohrozeným osobným údajom, identifikovať konkrétnych jednotlivcov alebo priradiť údaje k iným informáciám na identifikáciu jednotlivcov. V závislosti od okolností môže byť identifikácia možná priamo z porušených osobných údajov bez osobitného výskumu potrebného na odhalenie totožnosti jednotlivca, alebo môže byť mimoriadne náročné priradiť osobné údaje ku konkrétnemu jednotlivcovi, ale za určitých okolností by to stále mohlo byť možné. Identifikácia môže byť priamo alebo nepriamo možná z porušených údajov, môže však závisieť aj od konkrétneho kontextu porušenia a od verejnej dostupnosti súvisiacich osobných údajov. To môže byť relevantnejšie pre porušenia dôvernosti a dostupnosti.

Ako už bolo uvedené, osobné údaje chránené primeranou úrovňou šifrovania budú pre neoprávnené osoby nečitateľné bez kľúča na dešifrovanie. Navyše, riadne vykonaná pseudonymizácia (vymedzená v článku 4 ods. 5 ako „spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe“) môže takisto znížiť pravdepodobnosť identifikácie jednotlivcov v prípade porušenia. Nemožno však povedať, že vďaka samotným pseudonymizačným technikám sú údaje nezrozumiteľné.

- Závažnosť dôsledkov pre jednotlivcov

V závislosti od povahy osobných údajov, ktorých sa porušenie týka, napríklad osobitné kategórie údajov, možná ujma osobám, ku ktorej by mohol dôjsť, môže byť obzvlášť závažná, najmä pokiaľ by porušenie mohlo viesť ku krádeži totožnosti alebo podvodu, fyzickej ujme, psychickým ťažkostiam,

ponižovaniu alebo poškodeniu reputácie. Ak sa porušenie týka osobných údajov o zraniteľných osobách, mohli by byť vystavené väčšiemu riziku ujmy.

To, či si je prevádzkovateľ vedomý toho, že osobné údaje sú v rukách ľudí, ktorých zámery sú neznáme alebo možno zlé, môže mať vplyv na úroveň potenciálneho rizika. Ak sa osobné údaje poskytnú tretej strane podľa článku 4 ods. 10 alebo sa omylom poskytnú inému príjemcovi, môže dôjsť k porušeniu dôvernosti. To môže nastať napríklad vtedy, keď sa osobné údaje náhodou pošlú nesprávnemu oddeleniu organizácie alebo bežne využívanej dodávateľskej organizácii. Prevádzkovateľ môže požiadať príjemcu, aby buď vrátil alebo bezpečne zničil prijaté údaje. V oboch prípadoch, vzhľadom na to, že prevádzkovateľ má s príjemcom pretrvávajúci vzťah a môže poznať jeho postupy, históriu a iné dôležité údaje, možno tohto príjemcu považovať za „dôveryhodného“. Inými slovami, prevádzkovateľ má pri tomto príjemcovi určitú mieru istoty, takže môže primerane očakávať, že táto strana nebude čítať tieto údaje alebo pristupovať k týmto údajom, ktoré jej boli zaslané omylom, a že vyhovie pokynom prevádzkovateľa, aby ich vrátil. Dokonca aj v prípade prístupu k týmto údajom by prevádzkovateľ mohol mať dôveru voči príjemcovi, že s týmito údajmi nepodnikne žiadne kroky a ihneď ich vráti prevádzkovateľovi, a že bude spolupracovať pri ich vrátení. V takýchto prípadoch to možno zohľadniť v posúdení rizika, ktoré prevádzkovateľ vykoná po porušení – skutočnosť, že príjemca je dôveryhodný, môže odstrániť závažnosť dôsledkov porušenia, ale to neznamená, že k porušeniu nedošlo. To však zasa môže odstrániť pravdepodobnosť rizika pre jednotlivcov, a preto sa už nebude vyžadovať oznámenie dozornému orgánu alebo dotknutým osobám. Opäť to bude závisieť od individuálneho prípadu. Prevádzkovateľ napriek tomu musí uchovávať informácie týkajúce sa porušenia v rámci všeobecnej povinnosti uchovávať záznamy o porušeniach (pozri oddiel V ďalej).

Do úvahy by sa mala vziať aj trvalosť dôsledkov pre jednotlivcov, pričom vplyv možno považovať za väčší, ak sú dôsledky dlhodobé.

- Osobitné vlastnosti jednotlivca

Porušenie môže mať vplyv na osobné údaje týkajúce sa detí alebo iných zraniteľných osôb, ktoré v dôsledku toho môžu byť vystavené vyššiemu riziku ohrozenia. Môžu existovať aj iné faktory týkajúce sa jednotlivca, ktoré môžu ovplyvniť úroveň vplyvu, aký na nich má porušenie.

- Osobitné vlastnosti prevádzkovateľa

Povaha a úloha prevádzkovateľa a jeho činností môžu ovplyvniť úroveň rizika pre jednotlivcov v dôsledku porušenia. Napríklad zdravotnícka organizácia spracúva osobitné kategórie osobných údajov, čo znamená, že v prípade porušenia ochrany osobných údajov je hrozba pre jednotlivcov väčšia v porovnaní so zoznamom adries novín.

- Počet dotknutých osôb

Porušenie sa môže dotknúť jednej alebo niekoľkých osôb alebo aj niekoľko tisíc osôb, prípadne aj oveľa viac. Vo všeobecnosti platí, že čím je väčší počet dotknutých osôb, tým väčší vplyv môže mať porušenie. Porušenie však môže mať vážny vplyv aj len na jednu osobu, v závislosti od povahy osobných údajov a kontextu, v akom došlo k ich porušeniu. Základom je opäť zvážiť pravdepodobnosť a závažnosť vplyvu na dotknuté osoby.

- Všeobecné informácie

Preto pri posudzovaní rizika, ktoré pravdepodobne vyplýva z porušenia, by prevádzkovateľ mal zvážiť kombináciu závažnosti možného vplyvu na práva a slobody jednotlivcov a pravdepodobnosti výskytu. Je zrejmé, že ak sú dôsledky porušenia vážnejšie, riziko je vyššie a podobne ak je pravdepodobnosť ich výskytu väčšia, zvýši sa aj riziko. V prípade pochybností, by prevádzkovateľ nemal zbytočne neriskovať a mal by podať oznámenie. V prílohe B sa nachádzajú niektoré užitočné príklady rôznych typov porušení, ktoré zahŕňajú riziko alebo vysoké riziko pre jednotlivcov.

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) vypracovala odporúčania pre metodiku posudzovania závažnosti porušenia, ktorú môžu prevádzkovatelia a sprostredkovatelia považovať za užitočnú pri navrhovaní svojich plánov reakcie na porušenia[42].

V. Zodpovednosť a vedenie záznamov

A. Dokumentovanie porušení

Bez ohľadu na to, či je alebo nie je potrebné oznámiť porušenie dozornému orgánu, prevádzkovateľ musí viesť dokumentáciu všetkých porušení, ako sa vysvetľuje v článku 33 ods. 5:

> „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."

To súvisí so zásadou zodpovednosti podľa GDPR uvedenou v článku 5 ods. 2. Účel zaznamenávania porušení, ktoré nepodliehajú oznamovacej povinnosti, ako aj porušení, ktoré podliehajú oznamovacej povinnosti, sa vzťahuje aj na povinnosti prevádzkovateľa podľa článku 24, pričom dozorný orgán môže požiadať o nahliadnutie do týchto záznamov. Prevádzkovatelia sa preto vyzývajú, aby vytvorili interný register porušení, bez ohľadu na to, či sú povinní oznamovať alebo nie[43].

Hoci je na prevádzkovateľovi, aby určil, akú metódu a štruktúru používať pri dokumentovaní porušenia, pokiaľ ide o informácie, ktoré sú zapisovateľné, existujú kľúčové prvky, ktoré by mali byť prítomné vo všetkých prípadoch. Ako sa vyžaduje v článku 33 ods. 5, prevádzkovateľ musí zaznamenávať údaje týkajúce sa porušenia, ktoré by mali zahŕňať jeho príčiny, čo sa stalo a dotknuté osobné údaje. Mali by zahŕňať aj vplyvy a dôsledky porušenia spolu s opatreniami na nápravu prijatými prevádzkovateľom.

V GDPR sa nestanovuje obdobie uchovávania takejto dokumentácie. Ak takéto záznamy obsahujú osobné údaje, je úlohou prevádzkovateľa, aby určil primerané obdobie uchovávania v súlade so zásadami týkajúcimi sa spracúvania osobných údajov[44] a aby splnil zákonný základ pre spracúvanie[45]. Prevádzkovateľ musí uchovávať dokumentáciu v súlade s článkom 33 ods. 5, vzhľadom na to, že môže byť vyzvaný, aby dozornému orgánu poskytol dôkazy o dodržiavaní tohto článku resp. všeobecnejšie o dodržiavaní zásady zodpovednosti. Je zrejmé, že ak samotné záznamy neobsahujú žiadne osobné údaje, neuplatňuje sa zásada minimalizácie uchovávania[46] podľa GDPR.

Okrem týchto informácií pracovná skupina podľa článku 29 odporúča, aby prevádzkovateľ dokumentoval aj svoje odôvodnenie rozhodnutí prijatých v reakcii na porušenie. Najmä ak sa porušenie neoznámi, malo by sa zdokumentovať odôvodnenie tohto rozhodnutia. To by malo obsahovať dôvody, prečo sa prevádzkovateľ domnieva, že je nepravdepodobné, že by porušenie mohlo viesť k riziku pre práva a slobody jednotlivcov[47]. Prípadne ak sa prevádzkovateľ domnieva, že je splnená niektorá z podmienok článku 34 ods. 3, mal by byť schopný o tom poskytnúť primerané dôkazy.

---

42 ENISA, Odporúčania pre metodiku posúdenia závažnosti porušení ochrany osobných údajov, https://www.enisa.europa.eu/publications/dbn-severity.

43 Prevádzkovateľ sa môže rozhodnúť dokumentovať porušenia v rámci svojich záznamov o spracovateľských činnostiach, ktoré sú vedené podľa článku 30. Nevyžaduje sa samostatný register, a to za predpokladu, že informácie relevantné pre porušenie sú ako také jasne identifikovateľné a môžu sa získať na požiadanie.

44 Pozri článok 5.

45 Pozri článok 6 a článok 9.

46 Pozri článok 5 ods. 1 písm. e).

47 Pozri odôvodnenie 85.

Ak prevádzkovateľ oznámi porušenie dozornému orgánu, ale toto oznámenie je oneskorené, prevádzkovateľ musí byť schopný uviesť dôvody tohto oneskorenia; súvisiaca dokumentácia by mohla pomôcť preukázať, že oneskorenie oznámenia je odôvodnené a nie je neprimerané.

Ak prevádzkovateľ oznámi porušenie dotknutým osobám, mal by sa v súvislosti s porušením vyjadrovať transparentne a mal by ho oznámiť účinným a včasným spôsobom. Prevádzkovateľovi by teda pomohlo preukázať zodpovednosť a súlad uchovávaním dôkazov o takomto oznámení.

V záujme podpory dodržiavania článkov 33 a 34 by pre prevádzkovateľov aj sprostredkovateľov bolo výhodné mať zavedený postup dokumentovaného oznámenia, ktorým by sa stanovil postup, ktorý sa má dodržať v prípade odhalenia porušenia vrátane toho, ako zabrániť šíreniu incidentu, spravovať a riešiť incident, ako aj postup na posúdenie rizika a oznamovanie porušenia. V tejto súvislosti by na preukazovanie súladu s GDPR mohlo byť užitočné preukázať aj to, že zamestnanci boli informovaní o existencii takýchto postupov a mechanizmov a že vedia, ako reagovať na porušenia.

Treba poznamenať, že nedostatočné zdokumentovanie porušenia môže viesť k tomu, že dozorný orgán vykoná svoje právomoci podľa článku 58 alebo uloží správnu pokutu v súlade s článkom 83.

B. Úloha zodpovednej osoby

Prevádzkovateľ alebo sprostredkovateľ môžu mať zodpovednú osobu[48], buď podľa článku 37 alebo dobrovoľne z hľadiska osvedčených postupov. V článku 39 GDPR sa stanovuje niekoľko povinných úloh zodpovednej osoby, ale v prípade potreby sa nezabraňuje tomu, aby mu prevádzkovateľ pridelil ďalšie úlohy.

Úlohy zodpovednej osoby s osobitným významom pri oznamovaní porušení zahŕňajú okrem iných povinností aj povinnosť poskytovať poradenstvo a informácie v oblasti ochrany údajov prevádzkovateľovi alebo sprostredkovateľovi, monitorovať súlad s GDPR a poskytovať poradenstvo v súvislosti s posúdeniami vplyvu na ochranu údajov. Zodpovedná osoba musí okrem toho spolupracovať s dozorným orgánom a pôsobiť ako kontaktné miesto pre dozorný orgán a pre dotknuté osoby. Okrem toho treba poznamenať, že pri oznamovaní porušenia dozornému orgánu sa v článku 33 ods. 3 písm. b) vyžaduje, aby prevádzkovateľ poskytol meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta.

Pokiaľ ide o dokumentovanie porušení, prevádzkovateľ alebo sprostredkovateľ môže chcieť získať stanovisko svojej zodpovednej osoby k štruktúre, organizácii a správe tejto dokumentácie. Zodpovedná osoba by okrem toho mohla byť poverená vedením takýchto záznamov.

Tieto faktory znamenajú, že zodpovedná osoba by mala zohrávať kľúčovú úlohu pri napomáhaní pri predchádzaní porušeniu alebo príprave na porušenie prostredníctvom poskytovania poradenstva a monitorovania súladu, ako aj počas porušenia (teda pri oznamovaní dozornému orgánu) a počas každého ďalšieho vyšetrovania dozorným orgánom. V tejto súvislosti pracovná skupina podľa článku 29 odporúča, aby bola zodpovedná osoba ihneď informovaná o existencii porušenia a bola angažovaná počas celého procesu správy porušenia a oznamovania.

VI. Oznamovacie povinnosti podľa iných právnych nástrojov

Okrem oznamovania porušení podľa GDPR by si prevádzkovatelia a sprostredkovatelia mali navyše byť vedomí aj každej požiadavky na oznámenie bezpečnostných incidentov podľa iných súvisiacich právnych predpisov, ktoré sa na nich môžu vzťahovať a toho, či sa tým môže od nich vyžadovať, aby

[48] Pozri usmernenia pracovnej skupiny o zodpovedných osobách na tejto adrese: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

súčasne podali oznámenie o porušení ochrany osobných údajov dozornému orgánu. Takéto požiadavky sa môžu v jednotlivých členských štátoch líšiť, ale príklady požiadaviek na oznamovanie v iných právnych nástrojoch a to, ako tieto súvisia s GDPR, zahŕňajú:

- Nariadenie (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (nariadenie eIDAS)[49].

V článku 19 ods. 2 nariadenia eIDAS sa vyžaduje, aby poskytovatelia dôveryhodných služieb oznámili svojmu orgánu dohľadu narušenie bezpečnosti alebo integrity, ktoré má významný vplyv na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci nej. V prípade potreby, teda ak takéto narušenie alebo strata súčasne predstavujú porušenie ochrany osobných údajov podľa GDPR, by poskytovateľ dôveryhodných služieb mal podať oznámenie aj dozornému orgánu.

- Smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica NIS)[50].

V článkoch 14 a 16 smernice NIS sa vyžaduje, aby poskytovatelia základných služieb a poskytovatelia digitálnych služieb oznamovali bezpečnostné incidenty svojmu príslušnému orgánu. Ako sa uvádza v odôvodnení 63 smernice NIS[51], bezpečnostné incidenty môžu často zahŕňať porušenie ochrany osobných údajov. Zatiaľ čo v smernici NIS sa vyžaduje, aby príslušné orgány a dozorné orgány spolupracovali a vymieňali si informácie v tomto kontexte, stále platí, že ak takéto incidenty sú alebo sa stanú porušením ochrany osobných údajov podľa GDPR, od týchto prevádzkovateľov a/alebo poskytovateľov sa vyžaduje, aby o tom informovali dozorný orgán oddelene od požiadaviek na oznamovanie incidentov podľa smernice NIS.

Príklad

Poskytovateľ cloudových služieb, ktorý oznamuje porušenie podľa smernice NIS môže podať oznámenie aj prevádzkovateľovi, pokiaľ ide aj o porušenie ochrany osobných údajov. Podobne od poskytovateľa dôveryhodných služieb, ktorý podáva oznámenie podľa nariadenia eIDAS, sa môže vyžadovať, aby v prípade porušenia informoval príslušný orgán pre ochranu údajov.

- Smernica 2009/136/ES („smernica o právach občanov“) a nariadenie č. 611/2013 (nariadenie o oznámení porušenia).

Poskytovatelia verejne dostupných elektronických komunikačných služieb v kontexte smernice 2002/58/ES[52] musia oznamovať porušenia príslušným vnútroštátnym orgánom.

Prevádzkovatelia by si navyše mali byť vedomí všetkých ďalších právnych, zdravotných alebo odborných oznamovacích povinností podľa iných platných režimov.

---

49 Pozri https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32014R0910.

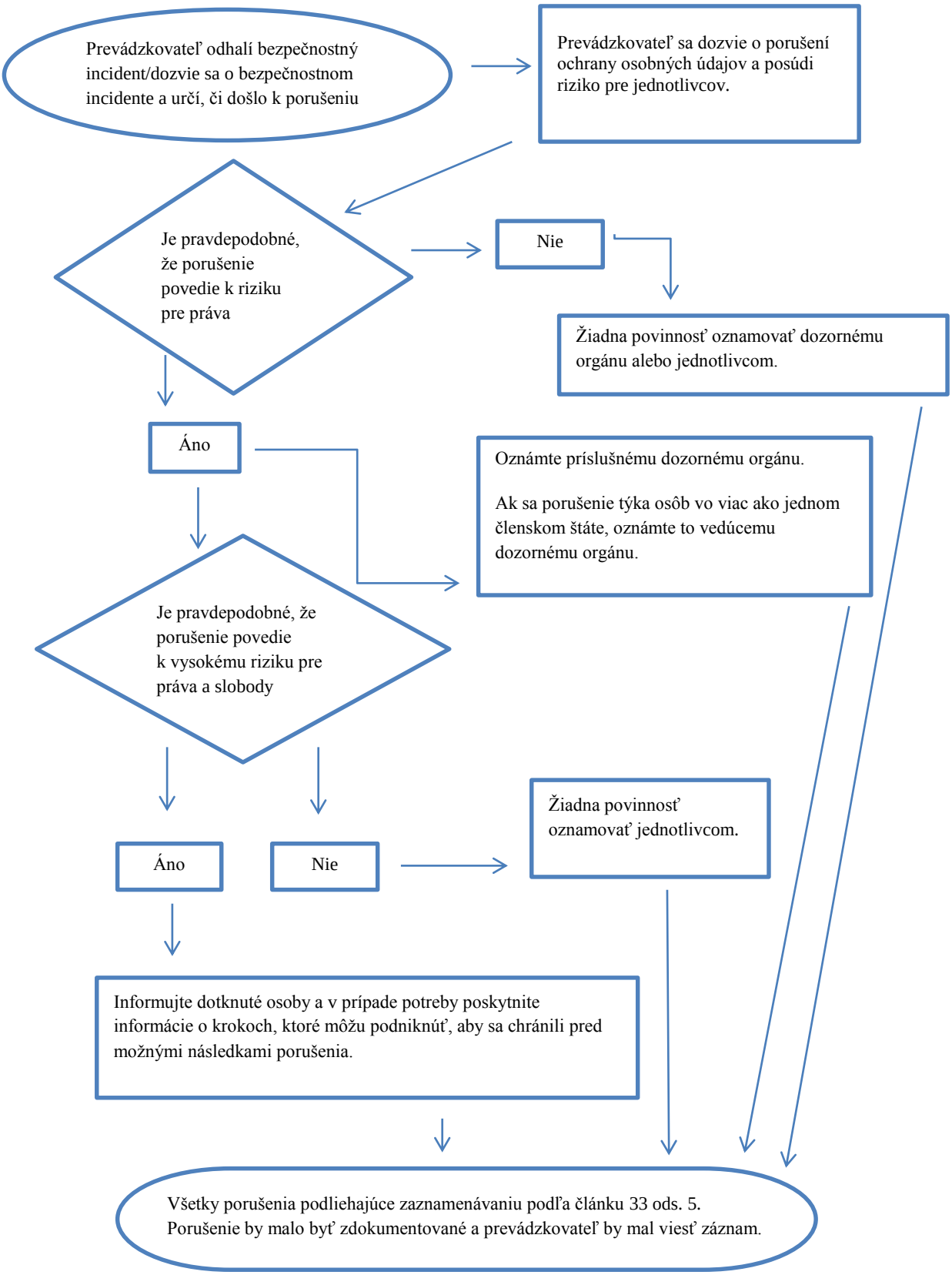
50 Pozrihttps://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016L1148.

51 Odôvodnenie 63: V *dôsledku incidentov je v mnohých prípadoch porušená ochrana osobných údajov. V tejto súvislosti by príslušné orgány a orgány na ochranu údajov mali navzájom spolupracovať a vymieňať si informácie o všetkých súvisiacich otázkach s cieľom riešiť akékoľvek prípady porušenia ochrany osobných údajov v dôsledku incidentov.“*

52 Európska komisia 10. januára 2017 navrhla nariadenie o súkromí a elektronických komunikáciách, ktorým sa nahradí smernica 2009/136/ES a zrušia požiadavky na oznamovanie. Až do schválenia tohto návrhu Európskym parlamentom však platia súčasné požiadavky na oznamovanie, pozri https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. **Príloha**

A. Vývojový diagram zobrazujúci požiadavky na oznamovanie



A. Príklady porušení ochrany osobných údajov a komu podávať oznámenia

Nasledujúce nevyčerpávajúce príklady pomôžu prevádzkovateľom pri určovaní toho, či je potrebné podávať oznámenie v rôznych scenároch porušení ochrany osobných údajov. Tieto príklady okrem toho môžu pomôcť rozlišovať medzi rizikom a vysokým rizikom pre práva a slobody jednotlivcov.

Príklad	**Oznámiť dozornému orgánu?**	**Oznámiť dotknutej osobe?**	**Poznámky/odporúčania**
i. Prevádzkovateľ uchovával zašifrovanú zálohu archívu osobných údajov na USB kľúči. Kľúč sa ukradne pri vlámaní.	Nie.	Nie.	Pokiaľ sú údaje zašifrované pomocou najmodernejšieho algoritmu a existujú zálohy údajov, jedinečný kľúč nie je porušený a údaje sa môžu včas obnoviť, nemusí ísť o porušenie podliehajúce oznámeniu. Ak sa však neskôr porušia, vyžaduje sa oznámenie.
ii. Prevádzkovateľ prevádzkuje online službu. V dôsledku kybernetického útoku na túto službu sa osobné údaje jednotlivcov stratia. Prevádzkovateľ má zákazníkov v jednom členskom štáte.	Áno, oznámte to dozornému orgánu, ak existujú pravdepodobné dôsledky pre jednotlivcov.	Áno, oznámte to jednotlivcom v závislosti od povahy dotknutých osobných údajov a od toho, či je závažnosť pravdepodobných dôsledkov pre jednotlivcov vysoká.	
iii. Krátky výpadok elektriny trvajúci niekoľko minút v call-centre prevádzkovateľa, čo znamená, že zákazníci sa nemôžu dovolať prevádzkovateľovi a získať prístup k svojim záznamom.	Nie.	Nie.	Toto nie je porušenie podliehajúce oznamovacej povinnosti, ale napriek tomu je incidentom, ktorý podlieha zaznamenávaniu podľa článku 33 ods. 5. Príslušné záznamy by mal viesť prevádzkovateľ.
iv. Prevádzkovateľ je napadnutý prostredníctvom softvéru ransomware, čo vedie k zašifrovaniu všetkých údajov. Nie sú dostupné žiadne zálohy a údaje sa nedajú obnoviť. Pri vyšetrovaní sa zistí, že jedinou funkciou softvéru ransomware bolo zašifrovanie	Áno, oznámte to dozornému orgánu, ak existujú pravdepodobné dôsledky pre jednotlivcov, keďže ide o stratu dostupnosti.	Áno, oznámte to jednotlivcom v závislosti od povahy dotknutých osobných údajov a od možného vplyvu nedostupnosti údajov, ako aj od iných možných dôsledkov.	Keby bola k dispozícii záloha a údaje by bolo možné včas obnoviť, nevyžadovalo by sa oznámenie dozornému orgánu alebo jednotlivcom, keďže by nedošlo k trvalej strate dostupnosti alebo dôvernosti. Keby sa však dozorný orgán dozvedel o incidente inými spôsobmi, mohol by

údajov a že v systéme sa nenachádza žiadny iný škodlivý softvér.			zvážiť vyšetrovanie s cieľom posúdiť súlad so širšími bezpečnostnými požiadavkami podľa článku 32.
v. Jednotlivec telefonuje do call-centra banky, aby nahlásil porušenie ochrany údajov. Jednotlivec dostal mesačný výpis z účtu určený pre niekoho iného. Prevádzkovateľ vykoná krátke vyšetrovanie (t. j. ukončené do 24 hodín) a s primeranou mierou spoľahlivosti určí, či došlo k porušeniu ochrany osobných údajov a či má systémovú chybu, ktorá môže znamenať, že aj iné osoby sú alebo by mohli byť dotknuté.	Áno.	Oznámenie sa podá len dotknutým osobám, ak existuje vysoké riziko a je jasné, že iné osoby neboli dotknuté.	Ak sa po ďalšom vyšetrovaní zistí, že bolo dotknutých viac osôb, dozornému orgánu sa musia poskytnúť najnovšie informácie a prevádzkovateľ prijme dodatočné opatrenie, teda informuje iné osoby, ak pre nich existuje vysoké riziko.
vi. Prevádzkovateľ prevádzkuje online trhovisko a má zákazníkov vo viacerých členských štátoch. Na trhovisko sa spácha kybernetický útok a útočník zverejní používateľské mená, heslá a históriu nákupov online.	Áno, informujte vedúci dozorný orgán, ak ide o cezhraničné spracúvanie.	Áno, keďže to môže viesť k vysokému riziku.	Prevádzkovateľ by mal podniknúť kroky, ako je nútená obnova hesiel dotknutých účtov, ako aj prijať ďalšie opatrenia na zmiernenie rizika. Prevádzkovateľ by mal vziať do úvahy aj všetky ostatné oznamovacie povinnosti, napríklad podľa smernice NIS ako poskytovateľ digitálnych služieb.
vii. Web-hostingová spoločnosť pôsobiaca ako sprostredkovateľ údajov identifikuje chybu v kóde, ktorý riadi autorizáciu používateľa. Dôsledkom chyby je, že každý používateľ má prístup k údajom o účte ktoréhokoľvek	Ako sprostredkovateľ musí web-hostingová spoločnosť bez zbytočného odkladu informovať svojich dotknutých klientov (prevádzkovateľov). Za predpokladu, že web-hostingová spoločnosť vykonala vlastné vyšetrovanie	Ak je pravdepodobné, že neexistuje žiadne vysoké riziko pre jednotlivcov, nie je potrebné im to oznámiť.	Web-hostingová spoločnosť (sprostredkovateľ) musí vziať do úvahy aj všetky ostatné oznamovacie povinnosti (napríklad podľa smernice NIS ako poskytovateľ digitálnych služieb). Ak neexistujú žiadne dôkazy o tejto

iného používateľa.	by dotknutí prevádzkovatelia mali mať primeranú istotu, či každý z nich utrpel porušenie, a preto ju možno považovať za pravdepodobne „vedomú“ po tom, čo boli prevádzkovatelia informovaní hostingovou spoločnosťou (sprostredkovateľom). Prevádzkovateľ to potom musí oznámiť dozornému orgánu.		zraniteľnosti zneužitej niektorým z jej prevádzkovateľov, nemuselo dôjsť k porušeniu podliehajúcemu oznamovacej povinnosti, ale je pravdepodobné, že ide o situáciu, ktorá podlieha zaznamenávaniu alebo o nedodržanie ustanovení článku 32.
viii. Zdravotné záznamy v nemocnici nie sú k dispozícii počas obdobia 30 hodín v dôsledku kybernetického útoku.	Áno, nemocnica je povinná to oznámiť, keďže to môže predstavovať vysoké riziko pre pohodu pacienta a jeho súkromie.	Áno, oznámte to dotknutým osobám.	
ix. Osobné údaje veľkého počtu študentov sa omylom odoslali na nesprávny zoznam adries s viac ako 1000 príjemcami.	Áno, oznámte to dozornému orgánu.	Áno, oznámte to jednotlivcom v závislosti od rozsahu a typu príslušných osobných údajov a od závažnosti možných dôsledkov.	
x. Email s priamym marketingom je odoslaný príjemcom v kolónke „komu:“ alebo „cc:“, takže každý príjemca môže vidieť emailovú adresu ostatných príjemcov.	Áno, oznámenie dozornému orgánu môže byť povinné, ak je dotknutý veľký počet jednotlivcov, ak sú odhalené citlivé údaje (napr. zoznam adries psychoterapeuta) alebo ak iné faktory predstavujú vysoké riziká (napr. pošta obsahuje vstupné heslá).	Áno, oznámte to jednotlivcom v závislosti od rozsahu a typu príslušných osobných údajov a od závažnosti možných dôsledkov.	Oznámenie nemusí byť potrebné, ak nie sú odhalené žiadne citlivé údaje a ak sa odhalí len malý počet emailových adries.