PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

18/CZ

WP250rev.01

Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679

přijaté dne 3. října 2017

naposledy revidované a přijaté dne 6. února 2018

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TYTO POKYNY:

OBSAH

ÚVOD

Obecné nařízení o ochraně osobních údajů (GDPR) zavádí požadavek, že jakékoli porušení zabezpečení osobních údajů (dále jen „porušení“) musí být oznámeno příslušnému vnitrostátnímu dozorovému úřadu[1] (nebo v případě přeshraničního porušení vedoucímu dozorovému úřadu) a že v některých případech musí být porušení oznámeno fyzickým osobám, jejichž osobních údajů se dané porušení týká.

Oznamovací povinnost v případě porušení mají v současnosti některé organizace, jako jsou například poskytovatelé veřejně dostupných služeb elektronických komunikací (ve smyslu směrnice 2009/136/ES a nařízení (EU) č. 611/2013)[2]. Některé členské státy EU již mají stanoveny své vlastní vnitrostátní oznamovací povinnosti v případě porušení. Mezi ně může patřit povinnost oznámit porušení týkající se kategorií správců spolu s poskytovateli veřejně dostupných služeb elektronických komunikací (například v Německu a v Itálii) nebo povinnost ohlašovat veškerá porušení týkající se osobních údajů (jako například v Nizozemsku). Jiné členské státy mohou mít příslušné kodexy správných postupů (například v Irsku[3]). Zatímco řada orgánů EU pro ochranu údajů v současnosti nabádá správce, aby porušení hlásili, směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů[4], kterou nařízení GDPR nahrazuje, neobsahuje konkrétní oznamovací povinnost, a proto bude takový požadavek pro mnohé organizace nový. Nařízení GDPR nyní stanoví, že všichni správci musí porušení oznamovat, ledaže je nepravděpodobné, že by dané porušení mohlo mít za následek riziko pro práva a svobody fyzických osob[5]. Zpracovatelé také hrají důležitou úlohu a každé porušení musí oznámit svému správci[6].

Pracovní skupina zřízená podle článku 29 se domnívá, že nový oznamovací požadavek má řadu výhod. Při vyrozumění dozorového úřadu mohou správci obdržet radu, zda je nutno informovat dotčené fyzické osoby. Dozorový úřad může správci skutečně nařídit, aby o porušení tyto osoby informoval[7]. Oznámení porušení dotčeným fyzickým osobám umožňuje správci poskytnout informace o rizicích, která hrozí v důsledku porušení, a také o krocích, které mohou tyto fyzické osoby podniknout, aby se ochránily před jeho možnými důsledky. Každý plán reakce na porušení by se měl zaměřit na ochranu fyzických osob a jejich osobních údajů. Oznámení o porušení je tudíž nutno považovat za nástroj zlepšující dodržování předpisů v souvislosti s ochranou osobních údajů. Zároveň je nutno poznamenat, že neoznámení porušení buď fyzické osobě, nebo dozorovému úřadu může znamenat, že se na správce může podle článku 83 vztahovat možná sankce.

---

[1] Viz čl. 4 odst. 21 nařízení GDPR.

[2] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:32009L0136 a http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32013R0611

[3] Viz https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046

[5] Práva zakotvená v Listině základních práv EU, k dispozici na adrese http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:12012P/TXT

[6] Viz čl. 33 odst. 2. Toto ustanovení je v zásadě podobné článku 5 nařízení (EU) č. 611/2013, který stanoví, že poskytovatel, který je smluvně zavázán, aby poskytl část služeb elektronických komunikací (bez přímého smluvního vztahu s účastníky), je v případě porušení zabezpečení osobních údajů povinen informovat smluvního poskytovatele.

[7] Viz čl. 34 odst. 4 a čl. 58 odst. 2 písm. e).

Správci a zpracovatelé se proto vyzývají, aby předem naplánovali a zavedli postupy, které jim umožní odhalit porušení a okamžitě na něj vhodně zareagovat s cílem omezit škody, posoudit riziko, které hrozí příslušným fyzickým osobám[8], a poté zjistit, zda je nutno informovat příslušný dozorový úřad, a v případě potřeby oznámit porušení dotčeným fyzickým osobám. Součástí tohoto plánu reakce na mimořádné události by mělo být vyrozumění dozorového úřadu.

Nařízení GDPR obsahuje ustanovení o tom, kdy je nutno porušení oznámit a komu a jaké informace se mají v rámci takového oznámení poskytovat. Informace, které mají být uvedeny v oznámení, lze poskytovat postupně, avšak v každém případě by správci měli na každé porušení reagovat včas.

Ve svém stanovisku č. 03/2014 k ohlašování případů porušení zabezpečení osobních údajů[9] poskytla pracovní skupina zřízená podle článku 29 pokyny správcům, aby jim pomohla při rozhodování, zda v případě porušení vyrozumět subjekty údajů. V rámci uvedeného stanoviska byla posouzena povinnost poskytovatelů služeb elektronických komunikací týkající se směrnice 2002/58/ES a byly poskytnuty příklady z několika různých odvětví v souvislosti s tehdejším návrhem nařízení GDPR a rovněž byly uvedeny osvědčené postupy pro všechny správce.

Tyto pokyny vysvětlují požadavky týkající se povinného oznamování případů porušení podle nařízení GDPR a popisují některé z kroků, jež mohou správci a zpracovatelé podniknout, aby tyto nové povinnosti splnili. Uvádějí rovněž příklady různých typů porušení a objasňují, koho je nutno v jednotlivých situacích vyrozumět.

I. Ohlašování případů porušení zabezpečení osobních údajů podle nařízení GDPR

A. Základní bezpečnostní aspekty

Jedním z požadavků nařízení GDPR je to, aby se za použití vhodných technických a organizačních opatření osobní údaje zpracovávaly takovým způsobem, který zajistí náležité zabezpečení osobních údajů, včetně ochrany před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením[10].

V souladu s tím nařízení GDPR požaduje, aby správci i zpracovatelé uplatňovali vhodná technická a organizační opatření k zajištění takové úrovně zabezpečení, která odpovídá riziku, jež zpracovávaným osobním údajům hrozí. Měli by přitom přihlédnout ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob[11]. Nařízení GDPR také požaduje zavedení veškeré odpovídající technologické ochrany a organizačních opatření, aby bylo možno okamžitě zjistit, zda došlo k porušení, což pak určuje, zda se uplatní oznamovací povinnost[12].

---

[8] To lze zajistit na základě požadavku na sledování a revizi v rámci posouzení vlivu na ochranu osobních údajů, který je nezbytný v případě takových operací zpracování, které by mohly vést k vysokému riziku pro práva a svobody fyzických osob (čl. 35 odst. 1 a 11).

[9] Viz Opinion 03/2014 on Personal Data Breach Notification (Stanovisko č. 03/2014 k ohlašování případů porušení zabezpečení osobních údajů) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Viz čl. 5 odst. 1 písm. f) a článek 32.

[11] Článek 32; viz také 83. bod odůvodnění.

[12] Viz 87. bod odůvodnění.

Klíčovým prvkem jakékoli politiky v oblasti bezpečnosti údajů je tudíž pokud možno zabránit porušení a v případě, že k němu i přesto dojde, reagovat na něj včas.

B. Co je porušení zabezpečení osobních údajů?

1. Definice

V rámci jakéhokoli pokusu řešit porušení by měl být správce nejprve schopen porušení rozpoznat. Nařízení GDPR definuje „porušení zabezpečení osobních údajů“ v čl. 4 odst. 12 jako:

> „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.

Co se rozumí pod pojmem „zničení“ osobních údajů, by mělo být zcela jasné: jedná se o situaci, kdy údaje již vůbec neexistují nebo již neexistují ve formě, která je pro správce jakkoli použitelná. Pojem „poškozené“ by měl být taktéž poměrně jasný: jedná se o situaci, kdy osobní údaje byly změněny, narušeny nebo již nejsou úplné. Výraz „ztráta“ je nutno v případě osobních údajů vykládat tak, že údaje sice ještě možná existují, ale správce nad nimi ztratil kontrolu, nemá k nim přístup nebo je již nemá ve svém držení. A konečně neoprávněné nebo protiprávní zpracování může zahrnovat zpřístupnění osobních údajů příjemcům, kteří nejsou oprávněni tyto údaje přijímat (nebo k nim mít přístup), (nebo přístup uvedených příjemců k těmto údajům), nebo jakoukoli jinou formu zpracování, která porušuje ustanovení nařízení GDPR.

Příklad

Příkladem ztráty osobních údajů může být situace, kdy zařízení obsahující kopii databáze zákazníků správce bylo ztraceno nebo odcizeno. Dalším příkladem ztráty může být situace, kdy jediná kopie souboru osobních údajů byla zašifrována ransomwarem nebo byla zašifrována správcem za použití klíče, který správce již nemá ve svém držení.

Mělo by být jasné, že porušení je druhem bezpečnostního incidentu. Jak však uvádí čl. 4 odst. 12, nařízení GDPR se vztahuje pouze na případy, kdy došlo k porušení zabezpečení *osobních údajů*. Důsledkem takového porušení je, že správce nebude schopen zajistit dodržování zásad zpracování osobních údajů uvedených v článku 5 nařízení GDPR. To poukazuje na rozdíl mezi bezpečnostním incidentem a porušením zabezpečení osobních údajů – zatímco v podstatě všechna porušení zabezpečení osobních údajů představují bezpečnostní incidenty, ne všechny bezpečnostní incidenty jsou nutně porušením zabezpečení osobních údajů[13].

Potenciální nepříznivé dopady porušení na fyzické osoby jsou uvedeny níže.

2. Typy porušení zabezpečení osobních údajů

Ve svém stanovisku č. 03/2014 k ohlašování případů porušení zabezpečení osobních údajů pracovní skupina zřízená podle článku 29 objasnila, že porušení lze kategorizovat podle následujících tří dobře známých zásad zabezpečení informací[14]:

[13] Je nutno poznamenat, že bezpečnostní incident není omezen na modely ohrožení, u nichž je útok na organizaci prováděn z vnějšího zdroje, ale zahrnuje i případy vnitřního zpracování, které porušují bezpečnostní zásady.

[14] Viz Stanovisko č. 03/2014.

- „porušení důvěrnosti“ – pokud dojde k neoprávněnému nebo náhodnému zveřejnění nebo zpřístupnění osobních údajů,
- „porušení integrity“ – pokud dojde k neoprávněnému nebo náhodnému pozměnění osobních údajů,
- „porušení dostupnosti“ – pokud dojde k náhodné nebo neoprávněné ztrátě přístupu[15] k osobním údajům nebo k jejich zničení.

Je také nutno uvést, že v závislosti na okolnostech se porušení může týkat zároveň důvěrnosti, integrity i dostupnosti osobních údajů, jakož i jakékoli kombinace těchto tří aspektů.

Zatímco určení, zda došlo k porušení důvěrnosti nebo integrity, je poměrně jasné, skutečnost, zda došlo k porušení dostupnosti, může být méně zřejmá. Porušení bude vždy považováno za porušení dostupnosti, pokud došlo k trvalé ztrátě nebo zničení osobních údajů.

Příklad

Mezi příklady ztráty dostupnosti patří situace, kdy byly údaje smazány, a to buď náhodně, nebo neoprávněnou osobou, nebo kdy v případě bezpečně zašifrovaných údajů došlo ke ztrátě dešifrovacího klíče. Pokud správce nedokáže obnovit přístup k údajům, například ze zálohy, považuje se to za trvalou ztrátu dostupnosti.

Ke ztrátě dostupnosti může dojít také v případě, že došlo k významnému narušení normální služby organizace, například při výpadku napájení nebo při útoku způsobujícím odepření služby, v jejichž důsledku jsou osobní údaje nedostupné.

Lze si položit otázku, zda dočasnou ztrátu dostupnosti osobních údajů považovat za porušení, a pokud ano, zda se jedná o porušení, které je nutno ohlásit. Článek 32 nařízení GDPR, který se týká „zabezpečení zpracování“, vysvětluje, že při provádění technických a organizačních opatření k zajištění úrovně zabezpečení odpovídající danému riziku je nutno mimo jiné zvažovat „schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování“ a „schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů“.

Bezpečnostní incident, v jehož důsledku se osobní údaje stanou na určitou dobu nedostupnými, je proto také určitým typem porušení, jelikož nemožnost přístupu k údajům může mít významný dopad na práva a svobody fyzických osob. Pro objasnění je nutno uvést, že pokud nejsou osobní údaje k dispozici z důvodu plánované údržby systému, nejedná se o „porušení zabezpečení“, jak je definováno v čl. 4 odst. 12.

Podobně jako v případě trvalé ztráty nebo zničení osobních údajů (nebo vlastně jakéhokoli jiného typu porušení) je porušení týkající se dočasné ztráty dostupnosti nutno zdokumentovat v souladu s čl. 33 odst. 5. To správci pomůže doložit odpovědnost dozorovému úřadu, který může požádat o

[15] Je dobře známo, že „přístup“ je v zásadě součástí „dostupnosti“. Viz například dokument NIST SP800-53rev4, který definuje „dostupnost“ jako: „Ensuring timely and reliable access to and use of information“ (zajištění včasného a spolehlivého přístupu k informacím a jejich využívání), k dispozici na adrese http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Dokument CNSSI-4009 také hovoří o: „Timely, reliable access to data and information services for authorized users“ (včasném, spolehlivém přístupu k datovým a informačním službám pro oprávněné uživatele). Viz https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Norma ISO/IEC 27000:2016 také definuje „dostupnost“ jako „Property of being accessible and usable upon demand by an authorized entity“ (vlastnost spočívající v tom, že jsou údaje dostupné a použitelné na vyžádání oprávněným subjektem): https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

předložení těchto záznamů[16]. V závislosti na okolnostech porušení však může nebo nemusí být nezbytné oznámit porušení dozorovému úřadu a dotčeným fyzickým osobám. Správce bude muset posoudit pravděpodobnost a závažnost dopadu na práva a svobody fyzických osob v důsledku nedostupnosti osobních údajů. Podle článku 33 bude muset správce porušení oznámit, ledaže je nepravděpodobné, že by porušení mohlo mít za následek riziko pro práva a svobody fyzických osob. Toto bude samozřejmě nutno posuzovat případ od případu.

Příklady

Pokud nejsou v případě nemocnice k dispozici, byť třeba jen dočasně, důležité zdravotní údaje o pacientech, mohlo by to představovat riziko z hlediska práv a svobod fyzických osob; v takovém případě může být například nezbytné zrušit operaci, čímž může být ohrožen pacientův život.

Naopak v případě, že jsou nedostupné systémy mediální společnosti po dobu několika hodin (např. kvůli výpadku dodávky elektrické energie), pokud tato společnost nemůže poté zasílat svým předplatitelům informační bulletiny, je nepravděpodobné, že by to představovalo riziko pro práva a svobody fyzických osob.

Je nutno poznamenat, že ačkoli ztráta dostupnosti systémů správce může být pouze dočasná a nemusí mít dopad na fyzické osoby, je důležité, aby správce zvážil všechny možné důsledky porušení, neboť jeho oznámení může být nezbytné z jiných důvodů.

Příklad

Napadení ransomwarem (škodlivý software, který zašifruje údaje správce a dešifruje je až do vyplacení výkupného) by mohlo vést k dočasné ztrátě dostupnosti, pokud lze údaje obnovit ze zálohy. Došlo však k průniku do sítě, takže může být nezbytné tuto událost oznámit, pokud je incident kvalifikován jako porušení důvěrnosti (to znamená, že útočník získal přístup k osobním údajům), což představuje riziko pro práva a svobody fyzických osob.

3. Možné důsledky porušení zabezpečení osobních údajů

Porušení může mít řadu významných nepříznivých dopadů na fyzické osoby, což může vést k fyzické, hmotné nebo nehmotné újmě. Nařízení GDPR objasňuje, že to může zahrnovat ztrátu kontroly fyzických osob nad jejich osobními údaji, omezení jejich práv, diskriminaci, krádež či zneužití totožnosti, finanční ztrátu, neoprávněné zrušení pseudonymizace, poškození dobrého jména a ztrátu důvěrnosti osobních údajů chráněných služebním tajemstvím. Může to rovněž zahrnovat jakékoli jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob[17].

V souladu s tím nařízení GDPR požaduje, aby správce oznámil porušení příslušnému dozorovému úřadu, ledaže není pravděpodobné, že by v jeho důsledku hrozil vznik takových nepříznivých účinků. Pokud existuje pravděpodobné vysoké riziko výskytu těchto nežádoucích účinků, nařízení GDPR požaduje, aby správce oznámil porušení dotčeným fyzickým osobám, jakmile je to proveditelné[18].

Důležitost schopnosti identifikovat porušení, posoudit riziko pro fyzické osoby a následně porušení oznámit, pokud je to nutné, je zdůrazněna v 87. bodě odůvodnění nařízení GDPR:

[16] Viz čl. 33 odst. 5.

[17] Viz také 75. a 85. bod odůvodnění.

[18] Viz také 86. bod odůvodnění.

„Mělo by být zjištěno, zda byla zavedena veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány. Skutečnost, že oznámení bylo provedeno bez zbytečného odkladu, se stanoví zejména s ohledem na povahu a závažnost daného porušení zabezpečení osobních údajů a jeho důsledky a nežádoucí účinky pro subjekt údajů. Toto oznámení může vést k zásahu dozorového úřadu v souladu s jeho úkoly a pravomocemi stanovenými v tomto nařízení."

Další pokyny ohledně posuzování rizika nežádoucích dopadů na fyzické osoby jsou uvedeny v oddílu IV.

Pokud správce neoznámí porušení zabezpečení údajů buď dozorovému úřadu, nebo subjektům údajů, nebo oběma těmto stranám, ačkoli jsou splněny požadavky článku 33 a/nebo článku 34, má dozorový úřad možnost volby, která musí zahrnovat zvážení všech nápravných opatření, jež má k dispozici, což by zahrnovalo posouzení možnosti uložit příslušnou správní pokutu[19], a to buď společně s nápravným opatřením podle čl. 58 odst. 2, nebo samostatně. Pokud je zvolena správní pokuta, může její výše činit až 10 milionů EUR nebo až 2 % z celkového celosvětového ročního obratu podniku podle čl. 83 odst. 4 písm. a) nařízení GDPR. Rovněž je důležité mít na paměti, že v některých případech by neoznámení porušení mohlo vést k odhalení buď neexistence stávajících bezpečnostních opatření, nebo jejich nedostatečnosti. V pokynech pracovní skupiny zřízené podle článku 29 ohledně správních pokut se uvádí: „Výskyt několika různých protiprávních jednání, ke kterým došlo společně v jakémkoli konkrétním jednotlivém případě, znamená, že dozorový úřad může uplatnit správní pokuty na úrovni, která je účinná, přiměřená a odrazující v mezích nejzávažnějšího protiprávního jednání". V takovém případě bude mít dozorový úřad rovněž možnost uložit sankce za neoznámení porušení (články 33 a 34) na straně jedné a za nepřítomnost (přiměřených) bezpečnostních opatření (článek 32) na straně druhé, jelikož se jedná o dvě samostatná protiprávní jednání.

II. Článek 33 – Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

A. Kdy porušení ohlásit

1. Požadavky podle článku 33

V čl. 33 odst. 1 se uvádí:

„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění."

V 87. bodě odůvodnění se uvádí[20]:

[19] Další podrobnosti naleznete v pokynech pracovní skupiny zřízené podle článku 29 k uplatňování a stanovení výše správních pokut, které jsou k dispozici na adrese: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Důležitý je zde rovněž 85. bod odůvodnění.

„Mělo by být zjištěno, zda byla zavedena veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány. Skutečnost, že oznámení bylo provedeno bez zbytečného odkladu, se stanoví zejména s ohledem na povahu a závažnost daného porušení zabezpečení osobních údajů a jeho důsledky a nežádoucí účinky pro subjekt údajů. Toto oznámení může vést k zásahu dozorového úřadu v souladu s jeho úkoly a pravomocemi stanovenými v tomto nařízení."

2. Jaký okamžik považovat za dobu, kdy se správce o porušení dozvěděl?

Jak je podrobně uvedeno výše, nařízení GDPR požaduje, aby správce případné porušení oznámil bez zbytečného odkladu a pokud možno nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděl. To může vyvolat otázku, jaký okamžik lze považovat za dobu, kdy se správce o porušení dozvěděl. Pracovní skupina zřízená podle článku 29 se domnívá, že za dobu, kdy se správce o porušení dozvěděl, by se měl považovat okamžik, kdy má správce dostatečnou jistotu, že došlo k bezpečnostnímu incidentu, který vedl k narušení zabezpečení osobních údajů.

Jak je však již uvedeno výše, nařízení GDPR vyžaduje, aby správce uplatňoval veškerou vhodnou technickou ochranu a organizační opatření, jež umožňují okamžitě zjistit, zda došlo k porušení, a neprodleně informovat dozorový úřad a subjekty údajů. Rovněž stanoví, že skutečnost, že oznámení bylo provedeno bez zbytečného odkladu, se stanoví zejména s ohledem na povahu a závažnost daného porušení zabezpečení osobních údajů a jeho důsledky a nežádoucí účinky pro subjekt údajů[21]. Tím vzniká povinnost správce zajistit, že se o případných porušeních dozví včas, aby mohl přijmout vhodná opatření.

Jaký přesný okamžik lze považovat za dobu, kdy se správce o konkrétním porušení dozvěděl, bude záviset na okolnostech daného porušení. V některých případech bude od počátku poměrně jasné, že došlo k porušení, zatímco v jiných případech může trvat nějakou dobu, než se zjistí, zda došlo k narušení zabezpečení osobních údajů. Důraz by však měl být kladen na okamžitá opatření k prošetření incidentu, aby se zjistilo, zda skutečně došlo k porušení zabezpečení osobních údajů, a pokud ano, je nutno přijmout nápravná opatření a porušení ohlásit, je-li to nutné.

Příklady

1. V případě ztráty USB úložiště s nezašifrovanými osobními údaji není často možné zjistit, zda k těmto údajům získaly přístup neoprávněné osoby. Nicméně ačkoli správce nemusí být schopen zjistit, zda došlo k porušení důvěrnosti, je nutno takový případ oznámit, protože existuje dostatečná míra jistoty, že došlo k porušení dostupnosti; za dobu, kdy se správce o daném porušení dozvěděl, se považuje okamžik, kdy si uvědomil, že došlo ke ztrátě USB úložiště.

2. Třetí strana informuje správce, že náhodou obdržela osobní údaje jednoho z jeho zákazníků, a poskytne důkaz o neoprávněném zveřejnění. Jelikož byly správci předloženy jasné důkazy o porušení důvěrnosti, nemůže být pochyb o tom, že se o porušení dozvěděl.

3. Správce odhalí, že možná došlo k proniknutí do jeho sítě. Zkontroluje své systémy, aby zjistil, zda došlo k narušení zabezpečení osobních údajů uchovávaných v tomto systému, a potvrdí, že tomu tak skutečně je. Opět platí, že jelikož má nyní správce jasné důkazy o porušení, nemůže být pochyb o tom, že se o porušení dozvěděl.

[21] Viz 87. bod odůvodnění.

4. Pachatel kybernetické kriminality se obrátí na správce poté, co napadl jeho systém, aby požádal o výkupné. V takovém případě má správce po kontrole svého systému, jíž si potvrdí, že byl skutečně napaden, jasný důkaz, že došlo k porušení, a není tudíž pochyb o tom, že se o něm dozvěděl.

Poté, co byl nejprve informován o možném porušení fyzickou osobou, mediální organizací nebo jiným zdrojem, nebo když sám odhalil bezpečnostní událost, může správce po krátkou dobu záležitost prošetřovat, aby zjistil, zda k porušení skutečně došlo. Po dobu tohoto prošetřování lze mít za to, že správce o porušení neví. Počáteční prošetření by však mělo začít co nejdříve a mělo by s přiměřeným stupněm jistoty určit, zda k porušení vůbec došlo; poté může následovat podrobnější vyšetřování.

Jakmile se správce o porušení dozví, musí porušení, na které se vztahuje ohlašovací povinnost, ohlásit bez zbytečného odkladu a pokud možno nejpozději do 72 hodin. Během této doby by měl správce posoudit pravděpodobné riziko pro fyzické osoby, aby určil, zda se má porušení oznámit, a aby stanovil opatření potřebná k řešení daného porušení. Správce však již může mít počáteční posouzení možného rizika, které by mohlo vyplývat z porušení, a to na základě posouzení vlivu na ochranu osobních údajů[22], které proběhlo před provedením dotyčné operace zpracování údajů. Avšak posouzení vlivu na ochranu osobních údajů může být obecnější ve srovnání s konkrétními okolnostmi jakéhokoli skutečného porušení, a proto bude v každém případě nezbytné provést další posouzení s přihlédnutím k těmto okolnostem. Podrobnější informace o posuzování rizika jsou uvedeny v oddílu IV.

Většinou by tato předběžná opatření měla být dokončena brzy po počátečním upozornění (tzn. když má správce nebo zpracovatel údajů podezření, že došlo k bezpečnostnímu incidentu, který se může týkat osobních údajů) – déle by to mělo trvat pouze ve výjimečných případech.

Příklad

Fyzická osoba informuje správce, že obdržela e-mail od někoho, kdo se vydává za správce, který obsahuje osobní údaje týkající se jeho (skutečného) používání služby správce, což naznačuje, že došlo k porušení zabezpečení správce. Správce po krátkou dobu incident prošetřuje a přitom zjistí proniknutí do své sítě a důkazy o neoprávněném přístupu k osobním údajům. Nyní by se mělo za to, že správce o porušení ví, a je nutno toto porušení oznámit dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení představovalo riziko pro práva a svobody fyzických osob. Správce bude muset přijmout vhodná nápravná opatření k vyřešení daného porušení.

Správce by proto měl mít zavedeny interní postupy, které mu umožňují porušení odhalit a vyřešit. Například ke zjištění některých nesrovnalostí ve zpracování údajů může správce nebo zpracovatel údajů používat určitá technická opatření, jako jsou analyzátory toku dat a protokolů, z nichž lze definovat události a výstrahy korelováním jakýchkoli dat protokolu[23]. V případě zjištění porušení je důležité toto porušení oznámit nadřízeným řídicím pracovníkům příslušné úrovně, aby bylo možno porušení vyřešit a pokud je to nutné, ohlásit ho podle článku 33 a v případě potřeby také podle článku 34. Taková opatření a mechanismy ohlašování by mohly být podrobně popsány ve správcových plánech reakce a/nebo postupech řízení. Ty správci pomohou efektivně plánovat a určit, kdo má v rámci organizace provozní odpovědnost za řešení daného porušení a jak nebo zda je nutno incident případně nahlásit nadřízeným.

[22] Viz pokyny pracovní skupiny zřízené podle článku 29 ohledně posouzení vlivu na ochranu osobních údajů, které jsou k dispozici na adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] Je nutno poznamenat, že data protokolu, která usnadňují auditovatelnost např. ukládání, úprav nebo vymazání údajů, lze rovněž považovat za osobní údaje týkající se osoby, která zahájila příslušnou operaci zpracování.

Správce by měl také mít uzavřena ujednání s veškerými zpracovateli, jejichž služeb využívá a kteří jsou sami povinni upozornit správce v případě porušení (viz níže).

Zatímco správcové a zpracovatelé jsou zodpovědní za zavedení vhodných opatření, která jim umožní porušením předcházet, reagovat na ně a řešit je, existují některé praktické kroky, které by měly být provedeny ve všech případech.

- Informace ohledně veškerých událostí týkajících se bezpečnosti by měly být směřovány k odpovědné osobě nebo osobám, které mají za úkol tyto incidenty řešit, zjišťovat existenci porušení a posuzovat riziko.
- Poté je nutno posoudit riziko pro fyzické osoby v důsledku porušení (pravděpodobnost nulového rizika, rizika nebo vysokého rizika), přičemž je nutno informovat příslušné útvary organizace.
- Je-li to zapotřebí, musí se porušení ohlásit dozorovému úřadu a případně oznámit i dotčeným fyzickým osobám.
- Zároveň by měl správce podniknout kroky, které zajistí, aby porušení způsobilo co nejméně škod, a přijmout opatření k nápravě.
- Průběžně by se mělo porušení dokumentovat.

Mělo by tudíž být zřejmé, že správce má povinnost jednat v případě jakéhokoli počátečního varování a zjistit, zda k porušení skutečně došlo. Toto krátké období umožňuje určité prošetření a správce během něho může shromažďovat důkazy a další důležité podrobnosti. Jakmile však správce s dostatečnou mírou jistoty zjistí, že k porušení došlo, potom v případě, že jsou splněny podmínky uvedené v čl. 33 odst. 1, musí porušení oznámit dozorovému úřadu bez zbytečného odkladu a pokud možno nejpozději do 72 hodin[24]. Pokud správce nekoná včas a přitom je zřejmé, že k porušení došlo, mohlo by to být považováno za neoznámení podle článku 33.

Článek 32 objasňuje, že správce a zpracovatel údajů by měli mít zavedena vhodná technická a organizační opatření k zajištění odpovídající úrovně zabezpečení osobních údajů: za základní prvky těchto opatření je nutno považovat schopnost porušení včas odhalit, reagovat na něj a ohlásit ho.

3. Společní správci

Článek 26 se týká společných správců a upřesňuje, že společní správci musí vymezit podíl každého z nich na odpovědnosti za dodržování nařízení GDPR[25]. To bude zahrnovat i určení toho, která strana bude odpovědná za splnění povinností podle článků 33 a 34. Pracovní skupina zřízená podle článku 29 doporučuje, aby smluvní ujednání mezi společnými správci obsahovala ustanovení, jež určují, který správce se ujme vedení, pokud jde o odpovědnost za dodržování povinností stanovených v nařízení GDPR ohledně ohlašování případů porušení.

4. Povinnosti zpracovatele

Správce si ponechává celkovou odpovědnost za ochranu osobních údajů, avšak zpracovatel hraje důležitou úlohu, která umožňuje správci splnit jeho povinnosti; součástí této úlohy je také ohlašování případů porušení. Ustanovení čl. 28 odst. 3 upřesňuje, že zpracování údajů zpracovatelem se řídí smlouvou nebo jiným právním aktem. V čl. 28 odst. 3 písm. f) se uvádí, že smlouva nebo jiný právní akt stanoví, že zpracovatel „je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici“.

[24] Viz nařízení č. 1182/71, kterým se určují pravidla pro lhůty, data a termíny, k dispozici na adrese: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:31971R1182&from=CS

[25] Viz také 79. bod odůvodnění.

Ustanovení čl. 33 odst. 2 objasňuje, že pokud správce využívá zpracovatele a zpracovatel zjistí porušení zabezpečení osobních údajů, které zpracovává jménem správce, musí porušení oznámit správci „bez zbytečného odkladu“. Je nutno poznamenat, že zpracovatel nemusí nejprve posoudit pravděpodobnost rizika vyplývajícího z porušení, než toto porušení oznámí správci; toto posouzení musí provést správce, jakmile se o porušení dozví. Zpracovatel musí pouze zjistit, zda k porušení došlo, a poté o něm informovat správce. Správce využívá zpracovatele k dosažení svých účelů, a proto by měl být v zásadě považován za osobu, která se o porušení dozvěděla, jakmile mu zpracovatel porušení oznámí. Povinnost zpracovatele informovat svého správce umožňuje správci porušení řešit a určit, zda je povinen porušení ohlásit dozorovému úřadu podle čl. 33 odst. 1 a dotčeným fyzickým osobám podle čl. 34 odst. 1. Správce by také mohl chtít porušení prošetřit, jelikož zpracovatel nemusí vědět o všech relevantních skutečnostech týkajících se této záležitosti, například zda má správce stále ve svém držení kopii či zálohu osobních údajů zničených nebo ztracených zpracovatelem. To může mít vliv na to, zda by správce musel následně porušení ohlásit.

Nařízení GDPR neuvádí výslovný časový limit, během kterého musí zpracovatel upozornit správce, kromě ustanovení, že tak musí učinit „bez zbytečného odkladu“. Pracovní skupina zřízená podle článku 29 proto doporučuje, aby zpracovatel neprodleně informoval správce a poté mu postupně poskytoval další informace o daném porušení, jakmile budou k dispozici další podrobnosti. To je důležité k tomu, aby správce mohl splnit požadavek, že musí porušení ohlásit dozorovému úřadu do 72 hodin.

Jak je vysvětleno výše, smlouva mezi správcem a zpracovatelem by měla stanovit, jakým způsobem by měly být vedle ostatních ustanovení nařízení GDPR splněny požadavky vyjádřené v čl. 33 odst. 2. To může zahrnovat požadavky na včasné vyrozumění zpracovatelem, které následně umožní zpracovateli splnit svou povinnost ohlásit porušení dozorovému úřadu do 72 hodin.

Pokud zpracovatel poskytuje služby více správcům, kteří jsou všichni dotčeni týmž incidentem, bude muset zpracovatel ohlásit podrobnosti incidentu každému správci.

Zpracovatel by mohl porušení ohlásit jménem správce, pokud mu k tomu správce dal řádné oprávnění a pokud je takový postup součástí smluvních ujednání mezi správcem a zpracovatelem. Takové ohlášení se musí provést v souladu s články 33 a 34. Je však důležité poznamenat, že právní odpovědnost za ohlašování má i nadále správce.

B. Poskytování informací dozorovému úřadu

1. Jaké informace je nutno poskytnout

Ohlášení případu porušení dozorovému úřadu správcem by podle čl. 33 odst. 3 mělo přinejmenším obsahovat:

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

Nařízení GDPR nedefinuje kategorie subjektů údajů ani záznamů osobních údajů. Pracovní skupina zřízená podle článku 29 však navrhuje, aby kategorie subjektů údajů odkazovaly na různé typy

fyzických osob, jejichž osobní údaje byly porušením dotčeny: v závislosti na použitých deskriptorech by výčet kategorií mohl zahrnovat mimo jiné například děti a jiné zranitelné skupiny, osoby se zdravotním postižením, zaměstnance nebo zákazníky. Podobně mohou kategorie záznamů osobních údajů odkazovat na různé typy záznamů, které může správce zpracovávat, jako jsou zdravotní údaje, záznamy o vzdělání, informace týkající se sociální péče, finanční údaje, čísla bankovních účtů, čísla pasů a podobně.

V 85. bodě odůvodnění je vysvětleno, že jedním z účelů ohlášení je omezit rozsah škod způsobených fyzickým osobám. Pokud tedy typy subjektů údajů nebo typy osobních údajů naznačují riziko vzniku konkrétních škod v důsledku porušení (např. krádež totožnosti, podvod, finanční ztrátu, ohrožení služebního tajemství), pak je důležité, aby byly tyto kategorie v ohlášení uvedeny. Tímto způsobem vzniká vazba na požadavek, že je nutno uvést popis pravděpodobných důsledků porušení.

Skutečnost, že přesné informace (např. přesný počet dotčených subjektů údajů) nejsou k dispozici, by neměla bránit včasnému ohlášení případu porušení. Podle nařízení GDPR je možno uvádět přibližný počet dotčených fyzických osob a počet příslušných záznamů osobních údajů. Pozornost by se měla zaměřit spíše na řešení nežádoucích účinků porušení než na poskytnutí přesných čísel. Jakmile je tedy zřejmé, že došlo k porušení, ale jeho rozsah ještě není znám, je postupné ohlašování (viz níže) bezpečným způsobem, jak splnit oznamovací povinnosti.

V čl. 33 odst. 3 se uvádí, že oznámení správce „musí přinejmenším obsahovat“ tyto informace, takže se správce může v případě potřeby rozhodnout uvést další podrobnosti. V případě různých typů porušení (porušení důvěrnosti, integrity nebo dostupnosti) může být nezbytné poskytnout další informace, aby bylo možné plně objasnit okolnosti každého případu.

Příklad

V rámci svého ohlášení dozorovému úřadu může správce považovat za užitečné uvést název zpracovatele údajů, pokud je tento hlavním původcem porušení, zvláště pokud porušení vedlo k incidentu, který se týká záznamů osobních údajů mnoha jiných správců, kteří vyžívají stejného zpracovatele.

Dozorový úřad si může v každém případě v rámci svého vyšetřování daného porušení vyžádat další podrobnosti.

2. Postupné ohlašování

V závislosti na povaze porušení může být nezbytné, aby správce provedl další šetření za účelem zjištění všech relevantních skutečností týkajících se dotyčného incidentu. Proto čl. 33 odst. 4 stanoví:

„Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu“.

Nařízení GDPR tedy uznává, že správci nemusí mít všechny potřebné informace týkající se daného porušení vždy k dispozici do 72 hodin od okamžiku, kdy se o něm dozvěděli, jelikož úplné a komplexní údaje o incidentu nemusí být během tohoto počátečního období vždy dostupné. Z toho vyplývá, že je možné postupné ohlašování. Je pravděpodobnější, že tomu tak bude v případě složitějších porušení, jako jsou některé typy incidentů v oblasti kybernetické bezpečnosti, kdy může být například nezbytné důkladné forenzní vyšetřování, aby se zcela stanovila povaha porušení a rozsah, v jakém bylo narušeno zabezpečení osobních údajů. V důsledku toho bude muset správce v mnoha případech později provádět další vyšetřování, následné sledování a opatřování dalších informací. To je přípustné, pokud správce uvede důvody pro zpoždění v souladu s čl. 33 odst. 1. Pracovní skupina zřízená podle článku 29 doporučuje, aby správce v rámci svého prvního ohlášení případu porušení dozorový úřad také případně informoval o tom, že dosud nemá k dispozici veškeré

potřebné informace a že další podrobnosti poskytne později. Dozorový úřad by měl odsouhlasit, jakým způsobem a mají být další informace poskytnuty. To správci nebrání poskytnout další informace v jakékoli jiné fázi, pokud se dozví o dalších relevantních podrobnostech ohledně daného porušení, které je nutno dozorovému úřadu poskytnout.

Účelem oznamovací povinnosti je podnítit správce k tomu, aby v případě porušení jednali neprodleně, okamžitě na něj vhodně zareagovali s cílem omezit škody a pokud možno obnovili narušené osobní údaje a aby si od dozorového úřadu vyžádali příslušné rady. Ohlášení případu porušení dozorovému úřadu během prvních 72 hodin může správci umožnit, aby se ujistil, že se správně rozhodl, pokud jde o ohlášení či neohlášení daného porušení dotčeným fyzickým osobám.

Účelem ohlášení případu porušení dozorovému úřadu však není pouze získat pokyny ohledně toho, zda vyrozumět dotčené fyzické osoby. V některých případech bude zřejmé, že kvůli povaze porušení a závažnosti rizika bude správce muset dotčené fyzické osoby bezodkladně informovat. Pokud například dojde k bezprostřední hrozbě krádeže totožnosti nebo ke zveřejnění zvláštních kategorií osobních údajů[26] na internetu, měl by správce bez zbytečného odkladu na porušení vhodně zareagovat s cílem omezit škody a oznámit ho dotčeným fyzickým osobám (viz oddíl III). Za výjimečných okolností k tomu může dojít dokonce ještě předtím, než správce porušení ohlásí dozorovému úřadu. Obecněji platí, že ohlášení případu porušení dozorovému úřadu nesmí sloužit jako zdůvodnění neoznámení daného porušení subjektu údajů v těch případech, kdy je to požadováno.

Mělo by rovněž být jasné, že po prvotním ohlášení by správce mohl dozorovému úřadu poskytovat postupně další podrobnosti, pokud následné vyšetřování odhalí důkazy o tom, že se podařilo eliminovat nepříznivé dopady daného bezpečnostního incidentu a že k žádnému porušení zabezpečení osobních údajů ve skutečnosti nedošlo. Tyto informace pak lze přidat k informacím, které již byly poskytnuty dozorovému úřadu, a incident příslušným způsobem zaznamenat jako událost, která nepředstavuje porušení zabezpečení osobních údajů. Za ohlášení incidentu, v jehož důsledku nakonec nedošlo k porušení zabezpečení osobních údajů, neexistuje žádná sankce.

Příklad

Správce do 72 hodin od zjištění porušení ohlásí dozorovému úřadu, že ztratil USB úložiště obsahující kopii osobních údajů některých jeho zákazníků. USB úložiště je později nalezeno v prostorách správce a jeho obsah je získán zpět. Správce o tom vyrozumí dozorový úřad a požádá o změnu dotyčného oznámení.

Je nutno poznamenat, že s postupným ohlašováním již počítá stávající stanovení povinností podle směrnice 2002/58/ES, nařízení (EU) č. 611/2013 a právní úprava jiných incidentů, které mají příslušné subjekty samy ohlašovat.

3. Opožděná ohlášení

Ustanovení čl. 33 odst. 1 jasně uvádí, že pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody zpoždění. Toto je spolu s pojetím postupného ohlašování výrazem uznání skutečnosti, že správce nemusí být vždy schopen oznámit porušení v této lhůtě a že může být přípustné i opožděné ohlášení.

Takový scénář by mohl nastat například v případě, že správce během krátkého časového období zaznamená více podobných porušení důvěrnosti, která stejným způsobem postihnou velký počet subjektů údajů. Správce se může dozvědět o porušení, a zatímco zahajuje své šetření, ještě před ohlášením zjistí další podobná porušení, jež mají odlišné příčiny. V závislosti na okolnostech může

[26] Viz článek 9.

správci určitou dobu trvat, než zjistí rozsah porušení, a než aby ohlašoval každé porušení jednotlivě, správce místo toho vypracuje smysluplné oznámení, ve kterém je uvedeno několik velmi podobných porušení s možnými rozdílnými příčinami. To by mohlo vést k tomu, že ohlášení dozorovému úřadu bude mít prodlení více než 72 hodin od okamžiku, kdy se správce poprvé o těchto porušeních dozvěděl.

Striktně řečeno, každé jednotlivé porušení je incidentem, který lze ohlásit. Aby správce nadměrně nezatěžoval dozorový úřad, může být schopen předložit „sdružené“ ohlášení, ve kterém jsou uvedena všechna tato porušení, za předpokladu, že se týkají stejného typu osobních údajů, jejichž zabezpečení bylo porušeno stejným způsobem během poměrně krátké doby. Pokud dojde k řadě porušení, která se týkají různých typů osobních údajů, jejichž zabezpečení bylo porušeno různými způsoby, mělo by se při ohlašování postupovat obvyklým způsobem, přičemž každé porušení je nutno ohlásit v souladu s článkem 33.

Ačkoli nařízení GDPR v určitém rozsahu povoluje opožděné ohlášení, nemělo by to být považováno za něco, k čemu dochází pravidelně. Je nutno poukázat na to, že sdružená ohlášení lze rovněž provádět v případě několika podobných porušení ohlášených do 72 hodin.

C. Přeshraniční porušení a porušení v provozovnách mimo EU

1. Přeshraniční porušení

V případě přeshraničního zpracování[27] osobních údajů může porušení postihnout subjekty údajů ve více než jednom členském státě. Ustanovení čl. 33 odst. 1 objasňuje, že pokud došlo k porušení, měl by jej správce ohlásit příslušnému dozorovému úřadu podle článku 55 nařízení GDPR[28]. V čl. 55 odst. 1 se uvádí:

> „Každý dozorový úřad je na území svého členského státu příslušný k plnění úkolů a výkonu pravomocí, které mu byly svěřeny v souladu s tímto nařízením“.

Avšak čl. 56 odst. 1 stanoví:

> „Aniž je dotčen článek 55, je dozorový úřad pro hlavní nebo jedinou provozovnu správce či zpracovatele příslušný k tomu, aby jednal jako vedoucí dozorový úřad v případě přeshraničního zpracování prováděného tímto správcem či zpracovatelem v souladu s postupem stanoveným v článku 60“.

Kromě toho čl. 56 odst. 6 stanoví:

> „Provádějí-li správce či zpracovatel přeshraniční zpracování, je pro ně jediným příslušným orgánem vedoucí dozorový úřad“.

To znamená, že kdykoli dojde v souvislosti s přeshraničním zpracováním k porušení, které je nutno ohlásit, bude muset správce vyrozumět vedoucí dozorový úřad[29]. Proto při sestavování plánu reakce

---

[27] Viz čl. 4 odst. 23.

[28] Viz také 122. bod odůvodnění.

[29] Viz pokyny pracovní skupiny zřízené podle článku 29 pro identifikaci vedoucího dozorového úřadu správce nebo zpracovatele údajů, které jsou k dispozici na adrese http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

na porušení musí správce posoudit, který dozorový úřad je vedoucím dozorovým úřadem, kterému bude muset porušení ohlásit[30]. To správci umožní okamžitě na porušení zareagovat a splnit své povinnosti podle článku 33. Mělo by být jasné, že v případě porušení v souvislosti s přeshraničním zpracováním je nutno vyrozumět vedoucí dozorový úřad, který nemusí být nutně tam, kde se dotčené subjekty údajů nacházejí, a dokonce ani tam, kde k porušení došlo. Při ohlašování případu porušení vedoucímu dozorovému úřadu by měl správce případně uvést, zda se porušení týká provozoven nacházejících se v jiných členských státech, a ve kterých členských státech se pravděpodobně nacházejí subjekty údajů, kterých se porušení týká. Pokud má správce pochybnosti o totožnosti hlavního dozorového úřadu, měl by případ ohlásit alespoň místnímu dozorovému úřadu tam, kde k porušení došlo.

2. Porušení v provozovnách mimo EU

Článek 3 se týká územní působnosti nařízení GDPR, včetně případů, kdy se vztahuje na zpracování osobních údajů správcem nebo zpracovatelem, který není usazen v EU. Čl. 3 odst. 2 zejména uvádí[31]:

> „Toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí:
>
> a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo
>
> b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie“.

Důležitý je rovněž čl. 3 odst. 3, který uvádí[32]:

> „Toto nařízení se vztahuje na zpracování osobních údajů správcem, který není usazen v Unii, ale na místě, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného“.

Pokud se na správce, který není usazen v EU, vztahuje čl. 3 odst. 2 nebo čl. 3 odst. 3 a dojde k porušení, má tudíž správce i nadále oznamovací povinnosti podle článků 33 a 34. Článek 27 požaduje, aby správce (a zpracovatel), pokud se na něho vztahuje čl. 3 odst. 2, určil svého zástupce v EU. V takových případech pracovní skupina zřízená podle článku 29 doporučuje ohlásit porušení dozorovému úřadu v tom členském státě, kde je usazen správcův zástupce v EU[33]. Podobně i zpracovatel, pokud se na něj vztahuje čl. 3 odst. 2, bude vázán povinnostmi týkajícími se zpracovatelů, přičemž v tomto případě je zejména důležitá povinnost ohlásit porušení správci podle čl. 33 odst. 2.

D. Situace, ve kterých se ohlášení nevyžaduje

Čl. 33 odst. 1 objasňuje, že porušení, u kterých „je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob“, není nutno ohlašovat dozorovému úřadu. Příkladem může být situace, kdy jsou osobní údaje již veřejně dostupné, a zveřejnění takových údajů tedy nepředstavuje pravděpodobné riziko pro dotčenou fyzickou osobu. To je v rozporu se stávajícími

[30] Přehled kontaktních údajů všech evropských vnitrostátních orgánů působících v oblasti ochrany údajů lze nalézt na adrese: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Viz také 23. a 24. bod odůvodnění.

[32] Viz také 25. bod odůvodnění.

[33] Viz 80. bod odůvodnění a článek 27.

požadavky ohledně ohlašování případů porušení, jež se vztahují na poskytovatele veřejně dostupných služeb elektronických komunikací, uvedenými ve směrnici 2009/136/ES, které stanoví, že všechna relevantní porušení je nutno ohlásit příslušnému orgánu.

Ve svém stanovisku č. 03/2014 k ohlašování případů porušení zabezpečení osobních údajů[34] pracovní skupina zřízená podle článku 29 objasnila, že porušení důvěrnosti osobních údajů, které byly zašifrovány pomocí nejmodernějšího algoritmu, je stále porušením zabezpečení osobních údajů a musí se ohlásit. Nicméně pokud je důvěrnost klíče neporušená – tzn. že zabezpečení klíče nebylo v případě jakéhokoli porušení bezpečnosti narušeno, a pokud byl klíč vytvořen tak, aby jej nikdo, kdo není oprávněn mít k tomuto klíči přístup, nemohl za použití dostupných technických prostředků zjistit – potom jsou dotyčné údaje v zásadě nerozluštitelné. Je tudíž nepravděpodobné, že by porušení mohlo mít nepříznivé dopady na dotčené fyzické osoby, a proto nemusí být těmto fyzickým osobám oznámeno[35]. Avšak i když jsou údaje zašifrované, jejich ztráta nebo pozměnění může mít nepříznivé důsledky pro subjekty údajů, jestliže správce nemá dostatečné zálohy těchto údajů. V takovém případě by bylo nezbytné porušení oznámit subjektům údajů i v případě, že by údaje samotné byly dostatečně zašifrované.

Pracovní skupina zřízená podle článku 29 rovněž vysvětlila, že by tomu tak bylo v případě, že by osobní údaje jako například hesla byly bezpečně hašovány i s použitím tzv. kryptografické soli, hašovaná hodnota by byla vytvořena pomocí nejmodernějších kryptografické hašovací funkce využívající šifrovací klíč, zabezpečení klíče použitého k hašování údajů by nebylo při žádném porušení narušeno a klíč použitý k hašování údajů by byl vygenerován způsobem, který nikdo, kdo není oprávněn mít k tomuto klíči přístup, nemůže za použití dostupných technických prostředků zjistit.

Pokud jsou tedy osobní údaje zabezpečeny tak, aby byly pro neoprávněné subjekty v podstatě nesrozumitelné, a pokud existují kopie nebo zálohy těchto údajů, nemusí být nutné ohlásit porušení důvěrnosti týkající se řádně zašifrovaných osobních údajů dozorovému úřadu. Je tomu tak proto, že takové porušení pravděpodobně nepředstavuje riziko pro práva a svobody fyzických osob. To samozřejmě znamená, že by nebylo nutno informovat ani dotčenou fyzickou osobu, neboť není pravděpodobné žádné vysoké riziko. Je však nutno mít na paměti, že i když zpočátku nemusí být ohlášení nutné, pokud pravděpodobně neexistuje žádné riziko pro práva a svobody fyzických osob, toto se může časem změnit a příslušné riziko by bylo nutno znovu posoudit. Pokud například později dojde k narušení zabezpečení šifrovacího klíče nebo se projeví slabé místo v zabezpečení šifrovacího softwaru, může být ohlášení dotyčného porušení nezbytné.

Kromě toho je nutno poznamenat, že pokud dojde k porušení v situaci, kdy neexistují zálohy zašifrovaných osobních údajů, jedná se o porušení dostupnosti, které by mohlo představovat rizika pro fyzické osoby, a proto může být nutné takový případ ohlásit. Podobně platí, že pokud dojde k porušení zahrnujícímu ztrátu zašifrovaných údajů, potom i když existuje záloha osobních údajů, může se i přesto jednat o porušení, které je nutno ohlásit, a to v závislosti na tom, jak dlouho trvalo obnovení údajů z této zálohy, a na dopadu, jaký měla nedostupnost údajů na dotčené fyzické osoby. Jak je uvedeno v čl. 32 odst. 1 písm. c), důležitým faktorem zabezpečení je „schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů“.

Příklad

[34] Viz stanovisko pracovní skupiny zřízené podle článku 29 č. 03/2014 k ohlašování případů porušení zabezpečení osobních údajů, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] Viz také čl. 4 odst. 1 a 2 nařízení (EU) č. 611/2013.

Porušením, které by nebylo nutné ohlásit dozorovému úřadu, by byla například ztráta bezpečně zašifrovaného mobilního zařízení využívaného správcem a jeho zaměstnanci. Za předpokladu, že šifrovací klíč zůstane v bezpečném držení správce a nejde o jedinou kopii osobních údajů, osobní údaje by byly pro útočníka nepřístupné. To znamená, že toto porušení pravděpodobně nepovede k riziku pro práva a svobody dotčených subjektů. Pokud se později ukáže, že došlo k narušení zabezpečení šifrovacího klíče nebo že šifrovací software či algoritmus jsou zranitelné, změní se tím riziko pro práva a svobody dotčených fyzických osob, a proto může být v takovém okamžiku nutné takový případ ohlásit.

Pokud však správce neoznámí porušení dozorovému úřadu v situaci, kdy údaje nebyly ve skutečnosti bezpečně zašifrovány, bude se jednat o nedodržení ustanovení článku 33. Proto by při výběru šifrovacího softwaru správci měli pečlivě zvážit kvalitu a správnou implementaci nabízeného šifrování, porozumět tomu, jakou úroveň ochrany skutečně poskytuje a posoudit, zda je to vzhledem k daným rizikům dostačující. Správci by rovněž měli být obeznámeni se specifiky způsobu, jakým jejich šifrovací produkt funguje. Určité zařízení může být například zašifrováno, když je vypnuté, ale nikoli v pohotovostním režimu. Některé produkty využívající šifrování mají „výchozí klíče“, které musí každý zákazník změnit, aby byly účinné. Šifrování může být také v současné době považováno odborníky v oblasti bezpečnosti za dostatečné, ale za několik let již může být zastaralé, což znamená, že je sporné, zda by údaje byly dotyčným produktem dostatečně zašifrovány a zda by takový produkt poskytoval odpovídající úroveň ochrany.

III. **Článek 34 – Oznamování případů porušení zabezpečení osobních údajů subjektu údajů**

A. Informování fyzických osob

V určitých případech je správce povinen nejen ohlásit porušení dozorovému úřadu, ale rovněž o něm vyrozumět dotčené fyzické osoby.

Čl. 34 odst. 1 stanoví:

„Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů“.

Správci by měli mít na paměti, že ohlášení případu porušení dozorovému úřadu je povinné, ledaže je nepravděpodobné, že by dané porušení mělo za následek riziko pro práva a svobody fyzických osob. Kromě toho, pokud je pravděpodobné, že v důsledku porušení existuje vysoké riziko pro práva a svobody fyzických osob, musí být informovány i dotčené fyzické osoby. Míra rizika, která určuje, kdy je nutno porušení oznámit fyzickým osobám, je tedy vyšší než v případě ohlašování dozorovým úřadům, a tudíž ne všechna porušení bude nutno oznamovat dotčeným fyzickým osobám, což je chrání před obtěžováním zbytečnými oznámeními.

Nařízení GDPR uvádí, že porušení je nutno oznámit fyzickým osobám „bez zbytečného odkladu“, což znamená co nejdříve. Hlavním účelem oznamování případů porušení fyzickým osobám je poskytnout konkrétní informace o krocích, jež by tyto osoby měly podniknout na svoji ochranu[36]. Jak je uvedeno

[36] Viz také 86. bod odůvodnění.

výše, v závislosti na povaze porušení a na hrozícím riziku pomůže včasné vyrozumění fyzickým osobám podniknout kroky, které je ochrání před nepříznivými důsledky porušení.

Příloha B těchto pokynů obsahuje orientační přehled příkladů, kdy může porušení pravděpodobně vést k vysokému riziku pro fyzické osoby, a tudíž případů, kdy bude muset správce porušení oznámit dotčeným fyzickým osobám.

B. Jaké informace je nutno poskytnout

Čl. 34 odst. 2 upřesňuje, že při oznamování případů porušení fyzickým osobám:

> „V oznámení určeném subjektu údajů podle odstavce 1 tohoto článku se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 33 odst. 3 písm. b), c) a d).“

Podle tohoto ustanovení by správce měl poskytnout alespoň tyto informace:

- popis povahy daného případu porušení,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa,
- popis pravděpodobných důsledků daného případu porušení a
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit daný případ porušení, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Jako příklad opatření přijatých k vyřešení případu porušení a ke zmírnění jeho možných nepříznivých dopadů by správce mohl uvést, že poté, co porušení ohlásil příslušnému dozorovému úřadu, obdržel rady ohledně toho, jak porušení zvládnout a zmírnit jeho dopady. Správce by měl případně rovněž poskytnout konkrétní rady dotčeným fyzickým osobám, aby se ochránily před možnými nepříznivými důsledky daného porušení, například že si mají nastavit nová hesla v případě, že došlo k narušení zabezpečení jejich přístupových údajů. Opět platí, že správce se může rozhodnout, že poskytne informace nad rámec toho, co je v takovém případě vyžadováno.

C. Kontaktování fyzických osob

V zásadě by se dané porušení mělo dotčeným subjektům údajů oznámit přímo, pokud to nevyžaduje vynaložení nepřiměřeného úsilí. V takovém případě by místo toho mělo být vydáno veřejné oznámení nebo přijato podobné opatření, kterým budou subjekty údajů informovány stejně účinným způsobem (čl. 34 odst. 3 písm. c)).

Při oznamování případů porušení subjektům údajů je nutno používat zprávy určené výhradně k tomuto účelu a tato oznámení by se neměla zasílat společně s jinými informacemi, jako jsou pravidelné aktualizace, informační bulletiny nebo standardní zprávy. To přispívá k tomu, aby oznámení daného případu porušení bylo jasné a transparentní.

Mezi příklady transparentních komunikačních metod patří přímé zasílání zpráv (například e-mail, SMS, přímá zpráva), výrazné bannery nebo oznámení na webových stránkách, poštovní zásilky a výrazné inzeráty v tištěných médiích. Oznámení, které se omezuje pouze na tiskovou zprávu nebo firemní blog, by nebylo účinným prostředkem pro oznámení případu porušení fyzické osobě. Pracovní skupina zřízená podle článku 29 doporučuje, aby správci zvolili takový prostředek, který maximalizuje pravděpodobnost řádného sdělení potřebných informací všem dotčeným fyzickým osobám. V závislosti na okolnostech to může znamenat, že správce místo jediného kontaktního kanálu využije několik různých komunikačních metod.

Může být rovněž nezbytné, aby správci zajistili přístupnost daného sdělení ve vhodných alternativních formátech a příslušných jazycích, aby se zajistilo, že dotčené fyzické osoby budou schopny

porozumět informacím, jež jim jsou poskytovány. Například při oznamování případu porušení fyzické osobě bude obecně vhodné použít jazyk, který byl používán při předchozím běžném styku s příjemcem. Pokud se však porušení týká subjektů údajů, s nimiž správce dosud nekomunikoval, nebo zejména s těmi, kteří mají bydliště v jiném členském státě nebo v jiné zemi, která není členem EU, než v zemi, kde je správce usazen, mohla by být přijatelná komunikace v místním národním jazyce s přihlédnutím k požadovanému zdroji. Klíčem je pomoci subjektům údajů pochopit povahu porušení a kroky, které mohou podniknout na svoji ochranu.

Správci mohou nejlépe určit nejvhodnější kontaktní kanál pro oznámení případu porušení fyzickým osobám, zejména pokud komunikují se svými zákazníky často. Avšak správce by zřejmě měl být opatrný, pokud jde o použití kontaktního kanálu, jehož zabezpečení bylo porušením narušeno, neboť tento kanál by také mohli použít útočníci, kteří se vydávají za správce.

Zároveň 86. bod odůvodnění vysvětluje, že:

> „Tato oznámení by měla být subjektům údajů učiněna, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů (například donucovacích orgánů). Například v případě potřeby zmírnit bezprostřední riziko způsobení újmy je nutné tuto skutečnost subjektům údajů neprodleně oznámit, zatímco v situaci, kdy je zapotřebí zavést vhodná opatření s cílem zabránit tomu, aby porušení zabezpečení osobních údajů pokračovalo nebo aby docházelo k podobným případům porušení, může být opodstatněna delší lhůta“.

Správci by proto mohli chtít kontaktovat dozorový úřad a případ s ním konzultovat, nejen aby získali rady ohledně informování subjektů údajů o porušení podle článku 34, ale také ohledně toho, jaké zprávy fyzickým osobám zaslat a jakým nejvhodnějším způsobem je kontaktovat.

S tím souvisí rada uvedená v 88. bodě odůvodnění, že při ohlašování případů porušení by měly být vzaty v úvahu „oprávněné zájmy donucovacích orgánů v případech, kdy by předčasné zpřístupnění mohlo zbytečně ztížit vyšetřování okolností porušení zabezpečení osobních údajů“. To může znamenat, že za určitých okolností, pokud to je odůvodněné, a na základě doporučení donucovacích orgánů, může správce oznámit porušení dotčeným fyzickým osobám později až v takovém okamžiku, aby to neovlivnilo příslušná vyšetřování. Po uplynutí této doby by však subjekty údajů musely být neprodleně informovány.

Kdykoli správce nemůže oznámit porušení některé fyzické osobě, protože nejsou k dispozici dostatečné údaje k jejímu kontaktování, měl by správce za těchto konkrétních okolností informovat dotčenou fyzickou osobu, jakmile je to proveditelné (např. když tato fyzická osoba uplatní své právo na přístup k osobním údajům podle článku 15 a poskytne správci své kontaktní údaje).

D. Podmínky, za kterých se oznámení nevyžaduje

Čl. 34 odst. 3 uvádí tři podmínky, při jejichž splnění není nutno dané porušení fyzickým osobám oznamovat. Jedná se o tyto podmínky:

- Správce před výskytem porušení uplatnil vhodná technická a organizační opatření k ochraně osobních údajů, zejména opatření, v jejichž důsledku jsou osobní údaje nesrozumitelné pro kohokoli, kdo není oprávněn mít k těmto údajům přístup. To by mohlo zahrnovat například ochranu osobních údajů pomocí nejmodernějšího šifrování nebo tokenizace.
- Okamžitě po porušení provedl správce kroky, které zajistí, že vysoké riziko pro práva a svobody fyzických osob se již pravděpodobně neprojeví. V závislosti na okolnostech případu mohl správce například okamžitě určit a podniknout kroky proti osobě, která získala přístup k osobním údajům ještě dříve, než s těmito údaji mohla něco udělat. Stále je třeba náležitě zohlednit případné důsledky jakéhokoli porušení důvěrnosti, a to opět v závislosti na povaze dotčených údajů.

- Kontaktovat dotčené fyzické osoby by vyžadovalo vynaložit nepřiměřené úsilí[37], třeba v případě, že jejich kontaktní údaje jsou v důsledku porušení ztraceny nebo nejsou vůbec známy. Například došlo k zaplavení skladu statistického úřadu vodou a dokumenty obsahující osobní údaje byly uloženy pouze v tištěné podobě. Místo toho musí správce vydat veřejné oznámení nebo přijmout podobné opatření, kterým budou fyzické osoby informovány stejně účinným způsobem. V případě nepřiměřeného úsilí by bylo možné uvažovat o technických opatřeních, která by umožnila poskytovat informace o porušení na vyžádání, což by se mohlo ukázat jako užitečné pro ty fyzické osoby, které mohou být porušením dotčeny, ale které správce nemůže jinak kontaktovat.

V souladu se zásadou odpovědnosti by správci měli být schopni dozorovému úřadu prokázat, že splňují jednu nebo více těchto podmínek[38]. Je nutno mít na paměti, že i když zpočátku nemusí být ohlášení nutné, pokud neexistuje žádné riziko pro práva a svobody fyzických osob, toto se může časem změnit a příslušné riziko bude nutno znovu posoudit.

Ustanovení čl. 34 odst. 4 vysvětluje, že pokud se správce rozhodne neoznámit porušení dotčené fyzické osobě, může dozorový úřad požadovat, aby tak učinil, pokud se domnívá, že porušení pravděpodobně povede k vysokému riziku pro fyzické osoby. Nebo může usoudit, že jsou splněny podmínky čl. 34 odst. 3, kdy se oznámení daného porušení fyzickým osobám nevyžaduje. Jestliže dozorový úřad rozhodne, že rozhodnutí neoznámit porušení subjektům údajů není dostatečně podložené, může zvážit využití svých dostupných pravomocí a sankcí.

IV. **Posouzení rizika a vysokého rizika**

A. Riziko jako faktor, který určuje, zda se má porušení ohlásit

Ačkoli nařízení GDPR zavádí povinnost ohlašovat porušení, není to vyžadováno za všech okolností:

- porušení se musí ohlásit příslušnému dozorovému úřadu, ledaže je nepravděpodobné, že by mohlo vést k riziku pro práva a svobody fyzických osob.
- Oznámení případu porušení fyzickým osobám je nezbytné pouze tehdy, když je pravděpodobné, že bude mít za následek vysoké riziko pro jejich práva a svobody.

To znamená, že okamžitě po zjištění případu porušení je zásadně důležité, aby se správce nejen snažil na incident vhodně zareagovat s cílem omezit škody, ale měl by rovněž posoudit riziko, které by mohlo z něj vyplynout. Existují pro to dva důležité důvody: za prvé, znalost pravděpodobnosti a potenciální závažnosti dopadu na dotčenou fyzickou osobu pomůže správci podniknout účinné kroky k omezení škod a řešení daného případu porušení, a za druhé, pomůže mu určit, zda je nezbytné porušení ohlásit dozorovému úřadu a v případě potřeby dotčeným fyzickým osobám.

Jak je vysvětleno výše, porušení je nutno ohlásit, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob, a faktorem, který určuje, že je nutno porušení oznámit subjektům údajů, je to, zda dané porušení bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob. Toto riziko existuje, pokud porušení může vést k fyzické, hmotné nebo nehmotné újmě fyzických osob, u jejichž údajů bylo narušeno zabezpečení.

[37] Viz pokyny pracovní skupiny zřízené podle článku 29 ohledně transparentnosti, které se zabývají problematikou nepřiměřeného úsilí, k dispozici na adrese http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Viz čl. 5 odst. 2.

Mezi příklady takové újmy patří diskriminace, krádež nebo zneužití totožnosti, finanční ztráta a poškození dobrého jména. Pokud se porušení týká osobních údajů, které odhalují rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborových organizacích nebo které zahrnují genetické údaje, údaje o zdravotním stavu nebo o sexuálním životě, údaje týkající se rozsudků v trestních věcech, údaje o protiprávním jednání nebo o souvisejících bezpečnostních opatřeních, mělo by se mít za to, že k takové újmě pravděpodobně dojde[39].

B. Jaké faktory je nutno brát v úvahu při posuzování rizika

Nařízení GDPR ve svém 75. a 76. bodě odůvodnění objasňuje, že obecně při posuzování rizika je nutno zvážit jak pravděpodobnost, tak závažnost rizika pro práva a svobody subjektů údajů. Dále nařízení GDPR uvádí, že riziko by se mělo vyhodnotit na základě objektivního posouzení.

Je nutno poznamenat, že posouzení rizika pro práva a svobody lidí v důsledku porušení se soustředí na jiné druhy rizika než na riziko, které se zvažuje v rámci posouzení vlivu na ochranu osobních údajů)[40]. V rámci posouzení vlivu na ochranu osobních údajů se zvažují jak rizika zpracování údajů, které probíhá podle plánu, tak i rizika v případě porušení. Při zvažování možného porušení se obecně posuzuje pravděpodobnost, že k takovému porušení dojde, a újma subjektu údajů, která by z tohoto porušení mohla vyplývat; jinými slovy, jedná se o posouzení hypotetické události. Při skutečném porušení k této události již došlo, a tak se pozornost soustředí výhradně na výsledné riziko dopadu porušení na fyzické osoby.

Příklad

V posouzení vlivu na ochranu osobních údajů se uvádí, že navrhované použití určitého bezpečnostního softwarového produktu na ochranu osobních údajů by bylo vhodným opatřením k zajištění úrovně bezpečnosti, jež odpovídá riziku pro fyzické osoby, které by zpracování údajů jinak představovalo. Pokud by však bylo následně zjištěno nějaké slabé místo, změnila by se tím vhodnost daného softwaru k eliminaci rizika pro chráněné osobní údaje, a proto by bylo nutno toto riziko znovu vyhodnotit v rámci probíhajícího posouzení vlivu na ochranu osobních údajů.

Slabé místo produktu někdo později využije a dojde k porušení zabezpečení. Správce by měl posoudit konkrétní okolnosti porušení, dotčené údaje a potenciální úroveň dopadu na fyzické osoby, jakož i to, do jaké míry je pravděpodobné, že se toto riziko projeví.

Při posuzování rizika pro fyzické osoby v důsledku porušení by správce tudíž měl zvážit konkrétní okolnosti porušení, včetně závažnosti možného dopadu a pravděpodobnosti, že k němu dojde. Pracovní skupina zřízená podle článku 29 proto doporučuje, aby se při posouzení brala v úvahu následující kritéria[41]:

- Typ porušení

[39] Viz 75. bod odůvodnění a 85. bod odůvodnění.

[40] Viz pokyny pracovní skupiny zřízené podle článku 29 ohledně posouzení vlivu na ochranu osobních údajů, které jsou k dispozici na adrese: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[41] Ustanovení čl. 3 odst. 2 nařízení (EU) č. 611/2013 poskytuje pokyny ohledně faktorů, které je nutno vzít v úvahu v souvislosti s ohlašováním porušení v odvětví služeb elektronické komunikace, což může být užitečné v souvislosti s ohlašováním podle nařízení GDPR. Viz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:cs:PDF

Typ porušení, k němuž došlo, může mít vliv na úroveň rizika, které fyzickým osobám hrozí. Například porušení důvěrnosti, při němž byly zdravotní informace poskytnuty neoprávněným osobám, může mít pro fyzickou osobu jinou škálu důsledků, než porušení, při kterém došlo ke ztrátě zdravotních údajů fyzické osoby, a tyto údaje již nejsou k dispozici.

- Povaha, citlivost a objem osobních údajů

Při posuzování rizika je samozřejmě klíčovým faktorem typ a citlivost osobních údajů, jejichž zabezpečení bylo porušením narušeno. Obvykle platí, že čím jsou údaje citlivější, tím větší riziko újmy bude dotčeným lidem hrozit, nicméně je rovněž nutno vzít v úvahu i další osobní údaje, které již mohou být o subjektu údajů k dispozici. Například zveřejnění jména a adresy fyzické osoby za běžných okolností pravděpodobně nezpůsobí podstatnou újmu. Pokud se však skutečný rodič dozví jméno a adresu adoptivního rodiče, důsledky mohou být velmi závažné jak pro adoptivního rodiče, tak pro dítě.

Případy porušení týkající se zdravotních údajů, dokladů totožnosti nebo finančních údajů, jako jsou údaje kreditní karty, mohou způsobit újmu každý sám o sobě, ale pokud jsou tyto údaje využity společně, mohou sloužit ke krádeži totožnosti. Kombinace různých osobních údajů je obvykle citlivější než jen jeden osobní údaj.

Některé typy osobních údajů se mohou na první pohled zdát poměrně neškodné, nicméně je nutno pečlivě zvážit, co tyto údaje mohou o dotčené fyzické osobě vypovídat. Seznam zákazníků, kteří přijímají pravidelné dodávky, nemusí být zvlášť citlivý, ale tytéž údaje o zákaznících, kteří požádali o přerušení dodávek po dobu jejich dovolené, by byly užitečnou informací pro zločince.

Podobně platí, že malé množství vysoce citlivých osobních údajů může mít na fyzickou osobu velký dopad a velké množství podrobností může poskytnout větší škálu informací o této osobě. Také porušení, které se týká velkých objemů osobních údajů o mnoha subjektech údajů, může mít vliv na odpovídající velký počet fyzických osob.

- Snadnost zjištění totožnosti fyzických osob

Důležitým faktorem, který je nutno brát v úvahu, je to, jak snadné bude pro někoho, kdo má přístup k osobním údajům, jejichž zabezpečení bylo narušeno, zjistit totožnost konkrétních fyzických osob nebo porovnat získané údaje s jinými informacemi za účelem identifikace fyzických osob. V závislosti na okolnostech by identifikace mohla být možná přímo na základě osobních údajů získaných v důsledku porušení, aniž by ke zjištění totožnosti určité fyzické osoby bylo zapotřebí provádět důkladné šetření, nebo může být naopak velmi obtížné přiřadit osobní údaje k jednotlivé osobě, ale za určitých podmínek by to mohlo být stále možné. Identifikace může být přímo nebo nepřímo možná na základě údajů získaných v důsledku porušení, ale může také záviset na konkrétních okolnostech porušení a na veřejné dostupnosti souvisejících osobních údajů. To může být relevantnější u porušení důvěrnosti a dostupnosti.

Jak je uvedeno výše, osobní údaje chráněné vhodnou úrovní šifrování budou pro neoprávněné osoby bez dešifrovacího klíče nesrozumitelné. Navíc vhodně uplatněná pseudonymizace (definovaná v čl. 4 odst. 5 jako „zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“) může také snížit pravděpodobnost zjištění totožnosti fyzických osob v případě porušení zabezpečení jejich osobních údajů. Samotné pseudonymizační techniky však nelze považovat za dostatečný způsob, jak zajistit, aby byly údaje nesrozumitelné.

- Závažnost následků pro fyzické osoby

V závislosti na povaze osobních údajů, kterých se porušení týká, například v případě zvláštních kategorií údajů, může být potenciální újma způsobená dotčeným fyzickým osobám obzvláště závažná, a to zejména v případech, kdy by porušení mohlo vést ke krádeži nebo zneužití totožnosti, fyzické újmě, psychickému utrpení, ponížení nebo poškození dobré pověsti. Pokud se porušení týká osobních údajů o zranitelných osobách, mohly by být tyto osoby vystaveny většímu riziku újmy.

To, zda si je správce vědom, že osobní údaje jsou v rukou lidí, jejichž záměry jsou neznámé nebo možná i nebezpečné, může mít vliv na úroveň potenciálního rizika. Může dojít k porušení důvěrnosti, při kterém jsou osobní údaje omylem poskytnuty třetí straně, jak je definována v čl. 4 odst. 10, nebo jinému příjemci. To se může stát například v případě, že jsou osobní údaje nedopatřením zaslány nesprávnému oddělení organizace nebo běžně používané dodavatelské organizaci. Správce může příjemce požádat, aby obdržené údaje vrátil nebo je bezpečně zničil. V obou případech, vzhledem k tomu, že správce má s dotyčným příjemcem dlouhodobý vztah a může mít přehled o jeho postupech, historii a dalších relevantních podrobnostech, lze příjemce považovat za důvěryhodného. Jinými slovy, správce může mít u daného příjemce určitou míru jistoty, s níž může důvodně očekávat, že nedopatřením zaslané údaje nebude dotyčná strana číst ani k nim přistupovat a že se bude řídit pokyny ohledně jejich vrácení. Dokonce i v případě, že došlo k přístupu k takovým údajům, mohl by správce příjemci i přesto důvěřovat, že s nimi nepodnikne žádné další kroky, neprodleně je správci vrátí a bude s ním spolupracovat na jejich obnovení. V takových případech lze toto zohlednit při posuzování rizika, které správce po výskytu porušení provádí, přičemž skutečnost, že příjemce je důvěryhodný, může vést ke snížení závažnosti následků porušení, ale neznamená, že k porušení nedošlo. Může tím však zase zmizet pravděpodobnost rizika pro fyzické osoby, a proto již nebude nutno porušení ohlásit dozorovému úřadu ani dotčeným fyzickým osobám. Bude to však opět záviset případ od případu. Správce má nicméně stále povinnost uchovávat informace o porušení v rámci obecné povinnosti vést záznamy o případech porušení (viz oddíl V níže).

Je také nutno brát v úvahu trvalost důsledků pro fyzické osoby, přičemž dopad lze považovat za závažnější, pokud jsou účinky dlouhodobé.

- Zvláštní charakteristiky fyzické osoby

Porušení může narušit zabezpečení osobních údajů týkajících se dětí nebo jiných zranitelných osob, které mohou být v důsledku toho vystaveny většímu riziku. Mohou existovat i další faktory týkající se fyzické osoby, jež mohou mít vliv na to, jak velký dopad bude porušení na danou osobu mít.

- Zvláštní charakteristiky správce údajů

Povaha a úloha správce a jeho činnosti mohou ovlivnit míru rizika, které hrozí fyzickým osobám v důsledku porušení. Například zdravotnické zařízení bude zpracovávat zvláštní kategorie osobních údajů, což znamená, že při porušení zabezpečení jejich osobních údajů jsou fyzické osoby více ohroženy než například v případě seznamu adres předplatitelů novin.

- Počet dotčených fyzických osob

Porušení může mít vliv pouze na jednu či několik málo fyzických osob, nebo naopak i na několik tisíc, ne-li mnohem více osob. Obecně platí, že čím větší je počet dotčených osob, tím větší dopad může dané porušení mít. Porušení však může mít vážný dopad i na jednu fyzickou osobu, a to v závislosti na povaze osobních údajů a okolnostech, za nichž bylo jejich zabezpečení narušeno. Nejdůležitější opět je zvážit pravděpodobnost a závažnost dopadu na dotčené osoby.

- Všeobecné aspekty

Při posuzování rizika, které v důsledku porušení pravděpodobně vznikne, by správce měl zvážit kombinaci závažnosti potenciálního dopadu na práva a svobody fyzických osob a pravděpodobnosti, že k těmto dopadům dojde. Je zřejmé, že pokud jsou důsledky porušení závažnější, riziko je vyšší a

podobně je tomu i v případě větší pravděpodobnosti jejich výskytu. V případě pochybností by měl správce raději postupovat obezřetně a incident ohlásit. Příloha B uvádí některé užitečné příklady různých typů porušení s běžným nebo vysokým rizikem pro fyzické osoby.

Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) vydala doporučení ohledně metodiky posuzování závažnosti porušení, která může být správcům a zpracovatelům údajů užitečná při koncipování jejich plánu reakce na porušení[42].

V. Odpovědnost a vedení záznamů

A. Dokumentace případů porušení

Bez ohledu na to, zda je nebo není nutno porušení ohlásit dozorovému úřadu, musí správce vést dokumentaci všech porušení, jak vysvětluje čl. 33 odst. 5:

> „Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem“.

To souvisí se zásadou odpovědnosti podle nařízení GDPR, uvedenou v čl. 5 odst. 2. Účelem vedení záznamů o případech porušení, které není nutno ohlašovat, a rovněž o těch, které se ohlašovat musí, rovněž souvisí s povinnostmi správce podle článku 24, přičemž dozorový úřad si může tyto záznamy vyžádat k nahlédnutí. Správci by si proto měli vytvořit interní registr porušení, a to bez ohledu na to, zda jsou povinni dotyčné případy ohlašovat nebo nikoli[43].

Ačkoli je na správci, aby určil, jaký způsob a strukturu použít při dokumentaci porušení, pokud jde o informace, které je nutno zaznamenat, existují klíčové prvky, které se musí uvádět ve všech případech. Jak požaduje čl. 33 odst. 5, správce musí zaznamenat podrobnosti týkající se porušení a přitom by měl uvést jeho příčiny, co se stalo a dotčené osobní údaje. Záznam by měl rovněž obsahovat dopady a důsledky porušení spolu s nápravnými opatřeními přijatými správcem.

Nařízení GDPR nestanoví dobu uchovávání takové dokumentace. Pokud tyto záznamy obsahují osobní údaje, je povinností správce určit vhodnou dobu uchovávání údajů v souladu se zásadami týkajícími se zpracování osobních údajů[44] a splnit požadavek zákonnosti zpracování údajů[45]. Bude muset uchovávat dokumentaci v souladu s čl. 33 odst. 5 do té míry, že může být vyzván, aby dozorovému úřadu poskytl důkazy o dodržování uvedeného článku nebo obecněji zásady odpovědnosti. Pokud samotné záznamy neobsahují žádné osobní údaje, potom se zásada omezení uložení[46] podle nařízení GDPR samozřejmě neuplatní.

---

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (Doporučení ohledně metodiky posuzování závažnosti porušení zabezpečení osobních údajů), https://www.enisa.europa.eu/publications/dbn-severity

[43] Správce se může rozhodnout zdokumentovat porušení v rámci svých záznamů o činnostech zpracování údajů, které vede podle článku 30. Samostatný registr se nevyžaduje za předpokladu, že informace týkající se porušení jsou jako takové jasně identifikovatelné a lze je na vyžádání získat.

[44] Viz článek 5.

[45] Viz článek 6 a také článek 9.

[46] Viz čl. 5 odst. 1 písm. e).

Pracovní skupina zřízená podle článku 29 doporučuje, aby správce spolu s těmito podrobnostmi dokumentoval také odůvodnění svých rozhodnutí přijatých v reakci na porušení. Zejména v případě neohlášení daného porušení je nutno zdokumentovat zdůvodnění tohoto rozhodnutí. Záznam by měl obsahovat důvody, proč se správce domnívá, že je nepravděpodobné, že by dané porušení mohlo mít za následek riziko pro práva a svobody fyzických osob[47]. Nebo, pokud se správce domnívá, že je splněna některá z podmínek uvedených v čl. 34 odst. 3, měl by být schopen poskytnout přiměřené důkazy o tom, že tomu tak skutečně je.

Pokud správce porušení dozorovému úřadu oznámí, avšak se zpožděním, musí být schopen toto zpoždění odůvodnit. Dokumentace týkající se této skutečnosti by mohla pomoci prokázat, že zpoždění ohlášení je odůvodněné a není nepřiměřené.

Pokud správce oznamuje porušení dotčeným fyzickým osobám, mělo by být takové oznámení transparentní a účinně a včas sdělené. Uchování důkazů o takovém oznámení by správci pomohlo prokázat jeho odpovědnost a splnění příslušných povinností.

Za účelem lepšího dodržování článků 33 a 34 by bylo výhodné, aby jak správci, tak zpracovatelé údajů měli zaveden zdokumentovaný postup ohlašování a oznamování, který uvádí jednotlivé kroky, jež je nutno učinit poté, co bylo porušení zjištěno, a to včetně způsobu, jak incident zvládnout, spravovat a zajistit nápravu, a který stanoví způsob posouzení rizika a ohlášení případu porušení. V tomto ohledu by za účelem prokázání souladu s nařízením GDPR mohlo být rovněž užitečné prokázat, že zaměstnanci byli informováni o existenci takových postupů a mechanismů a že vědí, jak na porušení reagovat.

Je nutno poznamenat, že pokud není porušení řádně zdokumentováno, může dozorový úřad uplatnit své pravomoci podle článku 58 a/nebo uložit správní pokutu podle článku 83.

B. Úloha pověřence pro ochranu osobních údajů

Správce nebo zpracovatel mohou mít pověřence pro ochranu osobních údajů[48], buď na základě požadavku stanoveného článkem 37, nebo dobrovolně v rámci dobré praxe. Článek 39 nařízení GDPR stanoví pro pověřence pro ochranu osobních údajů řadu povinných úkolů, ale nebrání tomu, aby mu správce v případě potřeby zadával i další úkoly.

Zvláštní význam v souvislosti s ohlašováním případů porušení má skutečnost, že mezi povinné úkoly pověřence pro ochranu osobních údajů mimo jiných povinností patří také poskytovat správci nebo zpracovateli rady a informace ohledně ochrany údajů, sledovat soulad s nařízením GDPR a poskytovat rady v souvislosti s posouzením vlivu na ochranu osobních údajů. Pověřenec pro ochranu osobních údajů musí rovněž spolupracovat s dozorovým úřadem a působit jako kontaktní místo pro dozorový úřad a subjekty údajů. Je nutno také poznamenat, že čl. 33 odst. 3 písm. b) požaduje, aby při ohlašování případu porušení dozorovému úřadu správce poskytl jméno a kontaktní údaje svého pověřence pro ochranu osobních údajů nebo jiného kontaktního místa.

Pokud jde o dokumentování případů porušení, může správce nebo zpracovatel chtít získat stanovisko svého pověřence pro ochranu osobních údajů ohledně struktury, zavedení a správy této dokumentace. Pověřence pro ochranu osobních údajů lze rovněž navíc pověřit i vedením takových záznamů.

Tyto faktory znamenají, že pověřenec pro ochranu osobních údajů by měl hrát klíčovou úlohu při předcházení případům porušení nebo při přípravě na ně, a to tím, že poskytuje rady a kontroluje

[47] Viz 85. bod odůvodnění.

[48] Viz pokyny pracovní skupiny zřízené podle článku 29 ohledně pověřence pro ochranu osobních údajů, které jsou k dispozici na adrese: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

dodržování příslušných předpisů, jakož i při samotném výskytu porušení (tzn. při jeho ohlašování dozorovému úřadu) a také během následného vyšetřování incidentu dozorovým úřadem. V tomto ohledu pracovní skupina zřízená podle článku 29 doporučuje, aby byl pověřenec pro ochranu osobních údajů bezodkladně informován o existenci porušení a aby byl zapojen do celého postupu zvládání a ohlašování případů porušení.

VI. Ohlašovací povinnosti podle jiných právních nástrojů

Vedle povinnosti ohlašovat a oznamovat případy porušení podle nařízení GDPR a odděleně od této povinnosti by si správci měli být vědomi i případných požadavků týkajících se ohlašování bezpečnostních incidentů podle jiných souvisejících právních předpisů, které se na ně mohou vztahovat, a měli by vědět, zda to může také vyžadovat, aby porušení zabezpečení osobních údajů současně ohlásili i dozorovému úřadu. Tyto požadavky se mohou v jednotlivých členských státech lišit, nicméně k jiným právním nástrojům vyžadujícím ohlašování případů porušení a stanovujícím způsob jejich vzájemný vztah s nařízením GDPR patří například následující právní předpisy:

- Nařízení (EU) č. 910/2014o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS)[49].

Ustanovení čl. 19 odst. 2 nařízení o eIDAS vyžaduje, aby poskytovatelé služeb vytvářejících důvěru vyrozuměli svůj orgán dohledu o každém narušení bezpečnosti nebo ztrátě integrity, jež mají významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje. Tam, kde to přichází v úvahu – tzn. pokud je takové narušení nebo ztráta také porušením zabezpečení osobních údajů ve smyslu nařízení GDPR – měl by poskytovatel služby vytvářející důvěru také vyrozumět příslušných dozorový úřad.

- Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice o bezpečnosti sítí a informací)[50].

Články 14 a 16 směrnice o bezpečnosti sítí a informací vyžadují, aby provozovatelé základních služeb a poskytovatelé digitálních služeb informovali příslušné orgány o bezpečnostních incidentech. Jak je uvedeno v 63. bodě odůvodnění směrnice o bezpečnosti sítí a informací[51], při bezpečnostních incidentech může často docházet také k porušení ochrany osobních údajů. Zatímco směrnice o bezpečnosti sítí a informací vyžaduje, aby příslušné orgány a dozorové úřady v této souvislosti navzájem spolupracovaly a vyměňovaly si informace, stále platí, že pokud takové incidenty jsou nebo se stanou porušením zabezpečení osobních údajů ve smyslu nařízení GDPR, jsou tito provozovatelé a/nebo poskytovatelé povinni dozorový úřad vyrozumět bez ohledu na požadavky týkající se oznamování incidentů podle směrnice o bezpečnosti sítí a informací.

Příklad

Poskytovatel cloudových služeb, který oznamuje porušení podle směrnice o bezpečnosti sítí a informací, může být rovněž povinen incident oznámit správci, pokud při něm došlo i k porušení

[49] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

51 V 63. bodě odůvodnění se uvádí: *„V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V tomto ohledu by příslušné orgány a orgány pro ochranu osobních údajů měly spolupracovat a vyměňovat si informace o všech významných skutečnostech, aby řešily jakékoli porušení ochrany osobních údajů, k němuž v důsledku incidentů dochází“.*

zabezpečení osobních údajů. Podobně platí, že poskytovatel služeb vytvářejících důvěru, který oznamuje incident podle nařízení eIDAS, může být v případě porušení rovněž povinen informovat příslušný orgán pro ochranu údajů.

- Směrnice 2009/136/ES (směrnice o právech občanů) a nařízení (EU) č. 611/2013 (nařízení o ohlašování případů porušení).

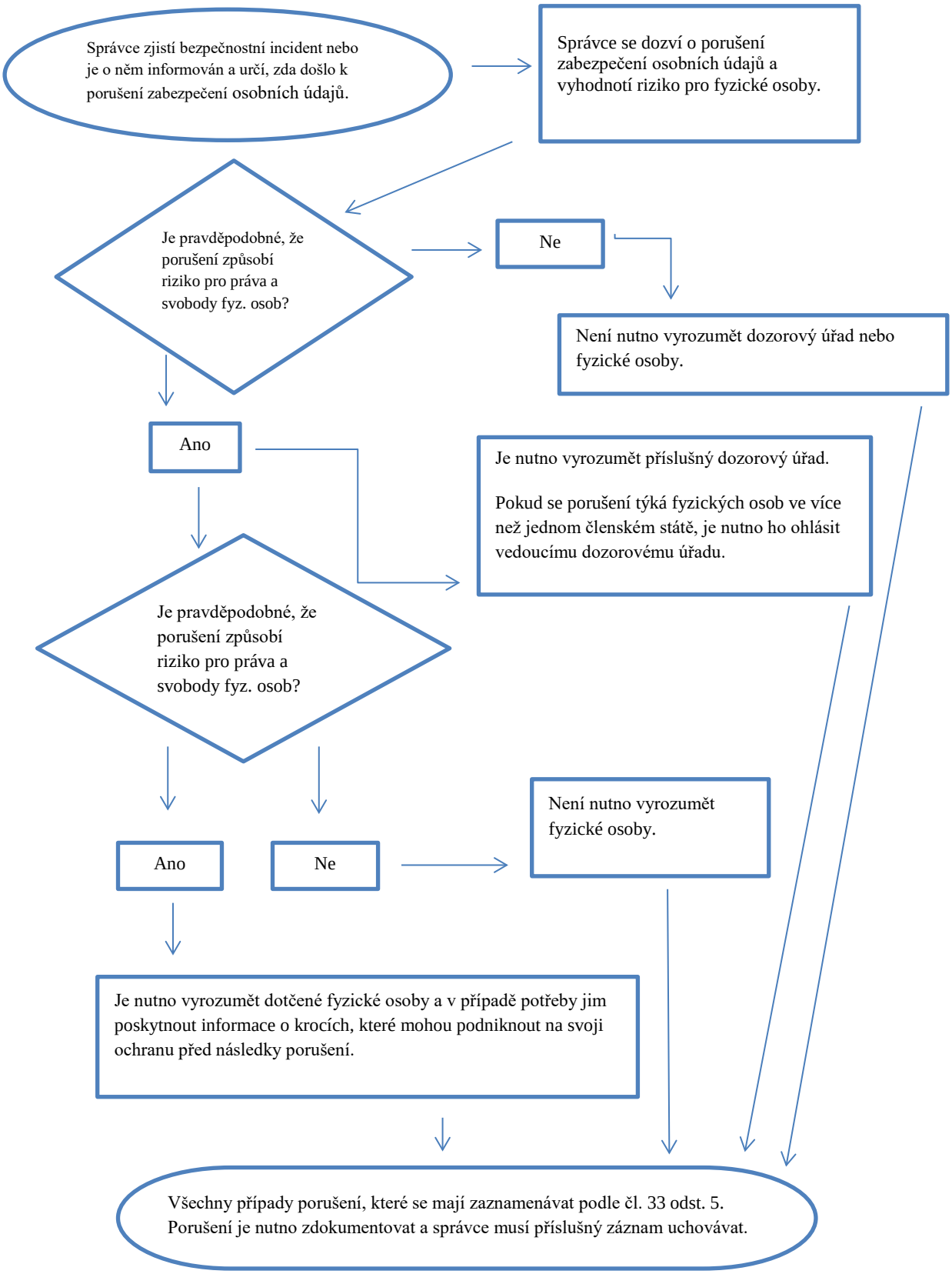
Poskytovatelé veřejně dostupných služeb elektronických komunikací ve smyslu směrnice 2002/58/ES[52] musí případy porušení oznamovat příslušným vnitrostátním orgánům.

Správci by také měli mít přehled o existenci případných dalších právních, lékařských nebo profesních oznamovacích povinností v rámci jiných platných režimů.

[52] Dne 10. ledna 2017 Evropská komise navrhla nařízení o soukromí a elektronických komunikacích, které nahradí směrnici 2009/136/ES a zruší požadavky týkající se oznamování. Dokud však tento návrh neschválí Evropský parlament, zůstává stávající oznamovací povinnost v platnosti, viz https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. **Příloha**

A. Vývojový diagram znázorňující požadavky týkající se ohlašování



B. Příklady porušení zabezpečení osobních údajů a koho o nich vyrozumět

Níže uvedený ilustrativní přehled příkladů pomůže správcům při rozhodování o tom, zda mají incident ohlásit při různých scénářích výskytu porušení zabezpečení osobních údajů. Tyto příklady mohou rovněž pomoci rozlišovat mezi běžným a vysokým rizikem pro práva a svobody fyzických osob.

Příklad	**Je nutno vyrozumět dozorový úřad?**	**Je nutno vyrozumět subjekt údajů?**	**Poznámky a doporučení**
i. Správce uložil zálohu archivu osobních údajů zašifrovaných na USB úložišti. Během vloupání dojde k odcizení úložiště.	Ne.	Ne	Pokud jsou údaje zašifrovány pomocí nejmodernějšího algoritmu, existují jejich zálohy, nebylo narušeno zabezpečení jedinečného klíče a údaje lze dostatečně rychle obnovit, nemusí se jednat o porušení, které je nutno ohlásit. Pokud však později dojde k narušení jejich zabezpečení, je nutno incident ohlásit.
ii. Správce provozuje online službu. V důsledku kybernetického útoku na tuto službu dojde k úniku osobních údajů fyzických osob. Správce má své zákazníky v jednom členském státě.	Ano, vyrozumějte dozorový úřad, pokud existuje pravděpodobnost důsledků pro fyzické osoby.	Ano, oznamte porušení fyzickým osobám v závislosti na povaze dotčených osobních údajů, a tehdy, pokud je závažnost pravděpodobných důsledků pro fyzické osoby vysoká.	
iii. V call centru správce dojde ke krátkému výpadku dodávky elektrického proudu, který trvá několik minut, takže zákazníci nemohou volat správce a mít přístup ke svým záznamům.	Ne.	Ne	Nejde o porušení, které se musí ohlásit, ale stále je to incident, který je nutno podle čl. 33 odst. 5 zaznamenat. Správce by měl uchovávat příslušné záznamy.
iv. Správce utrpí útok ransomwarem, který má za následek zašifrování všech údajů. Nejsou k dispozici žádné zálohy	Ano, vyrozumějte dozorový úřad, pokud existuje pravděpodobnost důsledků pro fyzické osoby, jelikož se jedná	Ano, vyrozumějte fyzické osoby v závislosti na povaze dotčených osobních údajů a možném dopadu nedostupnosti	Pokud by byla k dispozici záloha a údaje by bylo možno dostatečně rychle obnovit, není nutno tento incident ohlašovat dozorovému úřadu ani

a údaje nelze obnovit. Vyšetřování ukáže, že jedinou funkcí ransomwaru bylo zašifrování údajů a že v systému neexistuje žádný jiný škodlivý software.	o ztrátu dostupnosti.	údajů, jakož i na dalších pravděpodobných důsledcích.	oznamovat fyzickým osobám, protože by nedošlo k trvalé ztrátě dostupnosti nebo důvěrnosti. Pokud by se však dozorový úřad dozvěděl o incidentu jinými prostředky, může zvážit možnost provést šetření, aby posoudil soulad se širšími bezpečnostními požadavky článku 32.
v. Fyzická osoba zavolá do call centra banky, aby ohlásila porušení zabezpečení údajů. Osoba obdržela měsíční výpis z účtu někoho jiného. Správce provede krátké prošetření (tzn. takové, které dokončí během 24 hodin) a s přiměřenou mírou jistoty zjistí, zda skutečně došlo k porušení zabezpečení osobních údajů a zda se jedná o systémový nedostatek, který může znamenat, že jsou nebo mohou být dotčeny další osoby.	Ano.	Pokud existuje vysoké riziko a je zřejmé, že jiné osoby nebyly incidentem dotčeny, porušení se oznamuje pouze dotčeným fyzickým osobám.	Pokud se po dalším vyšetřování zjistí, že je dotčeno více fyzických osob, je nutno to ohlásit dozorovému úřadu a kromě toho správce oznámí porušení ostatním osobám, jestliže jim hrozí vysoké riziko.
vi. Správce provozuje internetové tržiště a má zákazníky ve více členských státech. Tržiště utrpí kybernetický útok a útočník zveřejní na internetu uživatelská jména, hesla a historii nákupů.	Ano, informujte vedoucí dozorový úřad, pokud se incident týká přeshraničního zpracování.	Ano, protože incident by mohl mít za následek vysoké riziko.	Správce by měl přijmout vhodná opatření, např. nucené přenastavení hesel dotčených účtů, jakož i další kroky ke zmírnění rizika. Správce by měl vzít v úvahu také případné další oznamovací povinnosti, např. podle směrnice o bezpečnosti sítí a informací jakožto poskytovatel digitálních služeb.

vii. Webhostingová firma působící jako zpracovatel údajů zjistí chybu v kódu, který řídí autorizaci uživatelů. V důsledku této chyby může každý uživatel přistupovat k podrobnostem účtu kteréhokoli jiného uživatele.	Jakožto zpracovatel musí webhostingová firma bez zbytečného odkladu vyrozumět své dotčené klienty (správce). Za předpokladu, že tato webhostingová firma provedla vlastní vyšetřování, měli by mít dotčení správci dostatečnou míru jistoty, zda každý z nich utrpěl porušení zabezpečení, a proto se bude pravděpodobně mít za to, že jakmile byli webhostingovou firmou (zpracovatelem) vyrozuměni, ví o dotyčném incidentu. Správce pak musí vyrozumět dozorový úřad.	Pokud fyzickým osobám pravděpodobně nehrozí vysoké riziko, není nutno jim incident oznamovat.	Webhostingová firma (zpracovatel) musí vzít v úvahu případné další oznamovací povinnosti (např. podle směrnice o bezpečnosti sítí a informací jakožto poskytovatel digitálních služeb). Pokud neexistují důkazy o tom, že by toto slabé místo bylo u některého z jejích správců zneužito, může to znamenat, že se nejedná o porušení, které je nutno ohlásit, avšak je pravděpodobné, že jde o incident, který se má zaznamenat, nebo který představuje nedodržení článku 32.
viii. V důsledku kybernetického útoku nejsou v nemocnici po dobu 30 hodin k dispozici zdravotní záznamy.	Ano, nemocnice je povinna incident ohlásit, jelikož může představovat vysoké riziko pro zdraví a soukromí pacienta.	Ano, incident je nutno oznámit dotčeným fyzickým osobám.	
ix. Osobní údaje velkého počtu studentů jsou nedopatřením odeslány do nesprávného seznamu zasílacích adres s více než 1000 příjemců.	Ano, incident je nutno ohlásit dozorovému úřadu.	Ano, vyrozumějte fyzické osoby v závislosti na rozsahu a typu osobních údajů a závažnosti možných důsledků.	
x. E-mailová zpráva pro účely přímého marketingu je zaslána příjemcům, kteří jsou všichni uvedeni v kolonce adresátů nebo příjemců kopie zprávy, takže každý příjemce vidí e-mailovou adresu ostatních příjemců.	Ano, ohlášení incidentu dozorovému úřadu může být povinné, pokud se týká velkého množství fyzických osob, pokud došlo k prozrazení citlivých údajů (např. seznam adres pacientů psychoterapeuta) nebo	Ano, vyrozumějte fyzické osoby v závislosti na rozsahu a typu osobních údajů a závažnosti možných důsledků.	Ohlášení nemusí být nutné, pokud nejsou prozrazeny žádné citlivé údaje a pokud je prozrazen jen malý počet e-mailových adres.

	pokud jiné faktory představují vysoké riziko (např. pokud zpráva obsahuje původní hesla).		