PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

WP250

Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679

Schváleno dne 3. října 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

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 a

s ohledem na svůj jednací řád,

PŘIJALA TATO VODÍTKA:

OBSAH

ÚVOD

Obecné nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“) zavádí požadavek, aby porušení zabezpečení osobních údajů (dále jen „porušení“ nebo „případ porušení“) bylo nahlášeno příslušnému národnímu dozorovému úřadu[1] a v jistých případech sdělit informaci o porušení jednotlivcům, jejichž osobní údaje byly tímto dotčeny.

Povinnost oznamovat porušení mají už nyní určité organizace, jako jsou poskytovatelé veřejně dostupných služeb elektronických komunikací (podle specifikace ve Směrnici 2009/136/ES a Nařízení (EU) č. 611/2013)[2]. V některých členských státech EU již povinnost ohlašovat porušení existuje. Může se jednat o povinnost nahlásit porušení postihující kromě poskytovatelů veřejně dostupných služeb elektronických komunikací také určité kategorie správců (například v Německu a Itálii) nebo povinnost oznámit veškerá porušení týkající se osobních údajů (Holandsko). V jiných zemích mohou existovat příslušné kodexy osvědčených postupů (například v Irsku[3]). V řadě členských států úřady vyzývají správce, aby porušení oznamovali, avšak Směrnice 95/46/ES[4], kterou nahradí Obecné nařízení, nestanovuje konkrétně povinnost ohlašovat porušení, a proto je tento požadavek pro mnoho organizací novinkou. Obecné nařízení vytváří z tohoto ohlašování povinnost pro všechny správce, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob[5]. Také zpracovatelé hrají důležitou roli a musí jakékoliv porušení nahlásit svému správci[6].

Pracovní skupina podle článku 29 (WP29) je toho názoru, že tato nová ohlašovací povinnost přináší mnoho výhod. Správci, poté co uvědomí dozorový úřad, mohou dostat radu, zda je potřeba informovat dotčené jednotlivce. Dozorový úřad vskutku může nařídit správci, aby tyto osoby informoval o případu porušení[7]. Sdělení o porušení jednotlivým osobám dává správcům možnost podat informaci o rizikách z porušení plynoucích a o krocích, které jednotlivec může podniknout k ochraně před těmito možnými důsledky. Jakýkoli plán reakce na porušení by měl být zaměřen na ochranu jednotlivců a jejich osobních údajů. Ohlašování případů porušení by tedy mělo být vnímáno jako nástroj k posílení souladu ve vztahu k ochraně osobních údajů. Současně je třeba zmínit, že neoznámení případu porušení, ať už jednotlivci nebo dozorovému úřadu, může podle článku 83 znamenat pro správce udělení pokuty.

Správci a zpracovatelé by proto měli s předstihem plánovat a zavést postupy umožňující odhalit a bezodkladně zvládnout případ porušení, posoudit riziko pro jednotlivce[8] a pak určit, zda je nutné vyrozumět příslušný dozorový úřad a případně i dotčené jednotlivce. Proces ohlášení dozorovému úřadu by měl být obsažen v plánu reakce na mimořádnou událost.

Obecné nařízení obsahuje ustanovení popisující, kdy případ porušení musí být ohlášen a komu a jaké informace by měly být za tímto účelem poskytnuty. Informace požadované v rámci ohlášení mohou být dodávány postupně, správci by však každopádně měli na případ porušení reagovat včas.

---

[1] Viz článek 4, odst. 21 Obecného nařízení

[2] Viz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 a http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX°/o3 A32013R0611

[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/ALL/?uri=celex%3A31995L0046

[5] Práva shrnutá v Listině základních práv Evropské unie: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:12012P/TXT&from=en

[6] Viz článek 33, odst. 2. Jde o podobný koncept jako v článku 5 Nařízení (EU) č. 611/2013, které uvádí, že poskytovatel, jenž je smluvně určen pro dodávku určité části služby elektronických komunikací (aniž by byl v přímém smluvním vztahu s uživateli) je povinen v případě narušení bezpečnosti osobních údajů uvědomit poskytovatele, s nímž má přímý smluvní vztah.

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

[8] To lze zajistit cestou posouzení vlivu na ochranu osobních údajů, které je vyžadováno pro operace zpracování, u nichž je pravděpodobné, že budou mít za následek vysoké riziko pro práva a svobody fyzických osob (Článek 35, odst. 1 a odst. 11.

Ve Stanovisku 03/2014 k ohlašování případů porušení zabezpečení osobních dat[9] nabídla WP29 správcům návod pro rozhodnutí, zda je případ porušení nutno oznámit subjektům údajů. Stanovisko zohledňuje povinnost poskytovatelů elektronických komunikací podle Směrnice 2002/58/ES a uvádí příklady z různých oblastí v kontextu tehdy ještě návrhu Obecného nařízení a předkládá správcům příklady osvědčených postupů.

Tato vodítka vysvětlují povinnost ohlašování případů porušení a požadavky na sdělované informace podle Obecného nařízení a také některé kroky, jež správci a zpracovatelé mohou podniknout ke splnění těchto nových povinností. Uvádějí rovněž příklady různých druhů porušení a koho, v tom kterém scénáři, je potřeba informovat.

I. Ohlašování **případů porušení zabezpečení podle Obecného nařízení**

A. Základní úvahy kolem bezpečnosti

Jeden z požadavků Obecného nařízení je, aby při použití patřičných technických a organizačních opatření byly osobní údaje zpracovány způsobem zajišťujícím náležité zabezpečení včetně ochrany před neoprávněným nebo protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením [10].

Co je míněno „zničením“ by mělo být zcela jasné: jde o případ, kdy údaje už neexistují vůbec nebo přinejmenším ne v podobě, aby byly správci k užitku. Pojem „poškození“ by také měl být poměrně jasný: je to případ, kdy osobní data byla pozměněna nebo už nejsou úplná. „Ztráta“ osobních údajů by měla být vykládána tak, že data sice mohou stále existovat, avšak správce nad nimi ztratil kontrolu nebo přístup k nim, či je už nemá v držení. A nakonec, neoprávněné nebo protiprávní zpracování může zahrnovat zpřístupnění osobních údajů příjemcům (nebo jejich přístup), kteří nemají oprávnění data získat (nebo mít k nim přístup) nebo jakoukoli jinou formu zpracování, která je v rozporu s Obecným nařízením.

Příklad

Příkladem ztráty osobních údajů může být zařízení obsahující kopii správcovy databáze zákazníků, kterou někdo ztratil nebo ukradl. Jiným příkladem ztráty může být jediná sada osobních údajů, která byla zašifrována vyděračským softwarem (ransomware) nebo správcem, jenž už nemá v držení příslušný klíč.

Obecné nařízení proto požaduje, aby správci i zpracovatelé disponovali náležitými technickými a organizačními opatřeními pro zajištění takové úrovně zabezpečení, která odpovídá riziku, jež dané zpracování osobních údajů doprovází. Měli by vzít v úvahu současný stav vývoje, náklady zavedení a povahu, rozsah, souvislosti a účely zpracování, stejně jako riziko proměnlivé pravděpodobnosti a závažnost pro práva a svobody fyzických osob[11]. Klíčovým prvkem jakékoliv politiky datové bezpečnosti je tedy schopnost případům porušení předcházet a pokud už k nim dojde, reagovat včas.

B. Co je porušení zabezpečení osobních údajů?

1. Definice

Správce musí případ porušení nejprve rozpoznat, aby vůbec byl schopen se jím zabývat. Obecné nařízení definuje „porušení zabezpečení osobních údajů "v článku 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“

[9] Viz Stanovisko 03/2014 k ohlašování případů porušení zabezpečení osobních dat: http://ec.europa.eu/iustice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

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

[11] Článek 32; viz také recitál 83

Jasné by mělo být, že případ porušení je druhem bezpečnostního incidentu. Podle článku 4, odst. 12 se však Obecné nařízení vztahuje na porušení zabezpečení pouze *osobních údajů.* Takové porušení má za následek, že správce nebude schopen zajistit soulad se zásadami zpracování osobních údajů podle článku 5 Obecného nařízení. To poukazuje na rozdíl mezi bezpečnostním incidentem a porušením zabezpečení osobních údajů – jednoduše řečeno, zatímco všechna porušení zabezpečení osobních dat jsou bezpečnostním incidentem, ne všechny bezpečnostní incidenty jsou nutně porušením zabezpečení osobních údajů.

Možné nepříznivé dopady případu porušení na jednotlivce jsou pojednány dále.

2. Typy porušení zabezpečení osobních údajů

Ve Stanovisku 03/2014 k ohlašování případů porušení zabezpečení osobních dat WP29 vysvětluje, že jednotlivá porušení mohou být zařazena do kategorií podle následujících tří dobře známých zásad informační bezpečnosti[12]:

- „Porušení důvěrnosti“ – v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.
- „Porušení dostupnosti“ – v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů.
- „Porušení integrity“ – v případě neoprávněného nebo náhodného pozměnění osobních údajů.

Rovněž je třeba mít na paměti, že porušení, v závislosti na okolnostech, se může dotýkat důvěrnosti, dostupnosti a integrity osobních údajů současně a stejně tak libovolné kombinace těchto faktorů.

Zatímco stanovení, zda došlo k porušení důvěrnosti nebo integrity, je poměrně jasné, odhalení případu porušení dostupnosti může být méně samozřejmé. Případ bude vždy považován za porušení dostupnosti, dojde-li k trvalé ztrátě nebo zničení osobních údajů.

Příklad

Příkladem ztráty dostupnosti může být smazání dat, buď náhodné nebo neoprávněnou osobou nebo, v případě bezpečně zašifrovaných dat, ztráta dešifrovacího klíče. Pokud správce není schopen obnovit přístup k datům, například ze záložního zařízení, pak je na tuto situaci nahlíženo jako na trvalou ztrátu dostupnosti.

Ztráta dostupnosti může také nastat v případě vážného narušení normálního chodu organizace, například z důvodu výpadku elektřiny nebo znemožnění uživatelského přístupu ke službě (útok DoS), v důsledku čehož se data stanou trvale nebo dočasně nedostupná.

Lze položit otázku, zda je dočasnou ztrátu dostupnosti možno považovat za porušení a pokud ano, jestli musí být ohlášena. Článek 32 Obecného nařízení s názvem „zabezpečení zpracování“ vysvětluje, že při provádění technických a organizačních opatření k zajištění úrovně zabezpečení odpovídající danému riziku, by mělo být přihlédnuto, mimo jiné, ke „schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování“ a „schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů“.

Incident, jehož následkem je dočasná nedostupnost osobních údajů, je proto porušením zabezpečení (a měl by být ohlášen[13]), byť, podle okolností, může nebo nemusí být vyžadováno ohlášení dozorovému úřadu a informování dotčených jednotlivců. Je-li pravděpodobné, že nedostupnost osobních údajů bude mít za následek riziko pro práva a svobody fyzických osob, pak správce musí provést ohlášení. Zde bude potřeba posuzovat případ od případu.

Příklady

V nemocnici by mohla nedostupnost kritických dat o pacientech, i jen dočasná, představovat riziko pro práva a svobody jednotlivce, například může být zrušena operace.

Naopak, budou-li po několik hodin nedostupné systémy v mediální firmě (např. kvůli výpadku proudu) a společnost nebude moci rozesílat newslettery svým abonentům, je nepravděpodobné, že by to představovalo nějaké riziko pro práva a svobody jednotlivce.

[12] Viz Stanovisko 03/2014
[13] Viz článek 33, odst. 5

Dále je třeba si uvědomit, že v případě ztráty dostupnosti systémů správce, jakkoliv pouze dočasné a nemající dopad na jednotlivce, už jen skutečnost, že došlo k narušení sítě, by stále mohla být považována za potenciální porušení důvěrnosti a bylo by požadováno ohlášení. Je proto důležité, aby správce vzal v úvahu veškeré možné důsledky případu porušení.

Příklad

Nákaza ransomwarem (vyděračský software, který zašifruje správcova data do doby, než obdrží výkupné) by mohla vést k dočasné ztrátě dostupnosti, pokud data nebude možné obnovit ze záložního zařízení. K narušení sítě však tak jako tak došlo a ohlášení by mohlo být vyžadováno, pokud by incident byl kvalifikován jako porušení důvěrnosti (tj. k osobním údajům měl přístup útočník) představující riziko pro práva a svobody jednotlivců.

3. Možné důsledky porušení zabezpečení osobních údajů

Porušení může mít celou řadu závažných nežádoucích účinků na jednotlivce, což může vyústit v tělesnou, materiální nebo nemateriální škodu. Obecné nařízení vysvětluje, že sem může patřit ztráta kontroly nad vlastními osobními údaji, omezení práv, diskriminace, krádež identity nebo podvod, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti a ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím. Může také zahrnovat jakékoliv jiné významné hospodářské nebo společenské znevýhodnění jednotlivců[14].

V souladu s tím požaduje Obecné nařízení po správcích, aby ohlásili porušení příslušnému dozorovému úřadu, vyjma případů, u nichž je nepravděpodobné, že by měly za následek takové nežádoucí účinky. Je-li pravděpodobné, že vysoké riziko těchto nežádoucích účinků existuje, pak podle Obecného nařízení musí správce případ porušení dotčeným jednotlivcům oznámit, jakmile to bude proveditelné[15].

Obecné nařízení v recitálu 87 vyzdvihuje, jak je důležitá schopnost odhalit případ porušení, vyhodnotit riziko pro jednotlivce a pak, je-li vyžadováno, ho ohlásit:

„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.“

Podrobnější návod k posouzení rizika nežádoucích účinků pro jednotlivce je v oddíle V.

Neohlásí-li správce dozorovému úřadu nebo subjektům údajů či oběma případ porušení zabezpečení, byť podmínky podle článků 33 a/nebo 34 byly naplněny, má dozorový úřad ke zvážení a na výběr všechna nápravná opatření, která má k dispozici, včetně udělení odpovídající správní pokuty, buď v doprovodu k nápravným opatřením podle článku 58, odst. 2 nebo samostatně. V případě správní pokuty může podle článku 83, odst. 4, písm. a) Obecného nařízení její výše dosáhnout až 10 000 000 eur nebo, jedná-li se o podnik, až 2 % celkového ročního obratu celosvětově. Dále je důležité mít na paměti, že v některých případech může neohlášení případu porušení odhalit buď absenci bezpečnostních opatření nebo jejich nedostatečnost. V takovém případě má dozorový úřad také možnost uložit sankce za nesplnění ohlašovací nebo oznamovací povinnosti (Články 33 a 34) na straně jedné a za absenci (odpovídajících) bezpečnostních opatření (Článek 32) na straně druhé, jelikož jde o dvě rozdílná porušení.

II. Článek 33 – Ohlašování dozorovému úřadu

A. Kdy ohlašovat

1. Požadavky dle článku 33

Článek 33, odst. 1 stanoví, že:

[14] Viz také recitály 85 a 75

[15] Viz také recitál 86.

„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.“

2. Co je okamžik, kdy se správce „dozvěděl“?

Jak je uvedeno výše, vyžaduje Obecné nařízení, aby, v případě porušení, správce toto porušení bez zbytečného odkladu ohlásil a, je-li to proveditelné, během 72 hodin od okamžiku, kdy se o něm dozvěděl. Zde může vyvstat otázka, jaký okamžik lze považovat za ten, kdy se správce „dozvěděl“ o porušení. WP29 se domnívá, že správce by měl být brán za „informovaného“, když má důvodný stupeň jistoty, že došlo k bezpečnostnímu incidentu vedoucímu k ohrožení osobních údajů. Bude to záviset na okolnostech konkrétního porušení. V některých případech bude hned zkraje poměrně jasné, že došlo k porušení, zatímco jindy může trvat nějaký čas, než se zjistí, že osobní data jsou ohrožena. Každopádně je třeba položit důraz na rychlé prošetření incidentu s cílem zjistit, zda skutečně došlo k porušení zabezpečení osobních údajů a pokud ano, přijmout nápravná opatření a, je-li to vyžadováno, případ ohlásit.

Příklady

V případě ztráty CD s nezašifrovanými daty není mnohdy možné zjistit, zda k nim získala přístup neoprávněná osoba. Takový případ však musí být ohlášen, neboť je tu dostatečná míra jistoty, že k porušení došlo; okamžikem, kdy se o něm správce dozvěděl, je chvíle, kdy si uvědomil ztrátu CD.

Třetí strana informuje správce, že nechtěně obdržela osobní data jednoho z jeho zákazníků a poskytne důkaz o neoprávněném zpřístupnění. Zde nemůže být pochyby, že správce se o případu „dozvěděl“, neboť mu byl předložen jasný důkaz.

Správce zjistí, že možná někdo proniknul do jeho sítě. Prověří tedy své systémy, zda osobní údaje v nich uložené nebyly ohroženy a v daném případě se jeho podezření potvrdí. Zde rovněž není pochyby o tom, že se správce o případu „dozvěděl“, jelikož v daném okamžiku o něm získal jasný důkaz.

Kybernetický zločinec kontaktuje správce poté, co se naboural do jeho systému za účelem vymáhání výkupného. Správce v tomto případě získal jasný důkaz o výskytu porušení a nezpochybnitelně „se o něm dozvěděl“.

Poté co byl o možném porušení informován jednotlivcem, přes média nebo z jiného zdroje, nebo pokud sám bezpečnostní incident odhalil, může správce po určitou krátkou dobu provádět šetření, aby zjistil, zda k porušení skutečně došlo. Během tohoto šetření nelze na správce pohlížet jako na informovaného. Očekává se však, že počáteční šetření začne co možná nejdříve a povede ke zjištění, s dostatečnou mírou jistoty, zda k porušení došlo a jaké to může mít důsledky pro jednotlivce; následovat pak může podrobnější šetření.

Nutnou součástí této reakce je jednak posouzení pravděpodobného rizika pro jednotlivce, jež porušení může mít za následek, s cílem stanovit, zda je nutno provést ohlášení, jednak kroky potřebné ke zvládnutí případu. Je však možné, že správce už prvotní posouzení možného rizika, které by porušení mohlo mít za následek, provedl v rámci posouzení vlivu na ochranu osobních údajů, vypracované před zahájením dotčené operace zpracování[16]. Posouzení vlivu však může být obecnější ve srovnání s konkrétními okolnostmi daného porušení, takže bude v každém případě nutno provést dodatečné posouzení zohledňující tyto skutečnosti. Více podrobností o posuzování rizika viz oddíl V.

Ve většině případů by tyto předběžné kroky měly být dokončeny záhy po prvním upozornění – trvat déle by měly jen ve výjimečných případech.

Příklad

Jednotlivec informuje správce, že obdržel e-mail, který vypadá jako odeslaný tímto správcem, a obsahující osobní údaje týkající se jeho užívání (skutečného) správcovy služby, což vede k domněnce, že na straně správce došlo

[16] Viz Pokyny WP29 pro posouzení vlivu: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

k narušení zabezpečení. Správce provede krátké šetření a zjistí průnik do jeho sítě a důkaz neoprávněného přístupu k osobním údajům. Správce bude od této chvíle považován za informovaného a bude muset případ ohlásit dozorovému úřadu, pokud je pravděpodobné, že bude mít za následek riziko pro jednotlivce. Správce bude muset přijmout náležitá nápravná opatření ke zvládnutí tohoto porušení.

Správce by tedy měl mít stanoveny vnitřní postupy k odhalování a zvládání případů porušení. Kupříkladu, pro objevení nesrovnalostí ve zpracování dat může správce nebo zpracovatel uplatnit určitá technická opatření, jako jsou analyzátory datových toků a logů, pomocí nichž je možné určit události a upozornění pomocí korelace logů[17]. Při zjištění případu porušení je důležité zpravit o něm vedení na odpovídající úrovni řízení, aby mohl být řešen a, pokud je požadováno, ohlášen v souladu s článkem 33 a, je-li nutné, s článkem 34. Taková opatření spolu s mechanismy informování by mohly být podrobně upraveny ve správcových plánech reakce na incidenty a/nebo v ujednáních o správě a řízení. Správci pomohou účinně plánovat a určit, kdo v organizaci má provozní odpovědnost za vyřizování případů porušení a jak nebo zda vůbec může incident eskalovat.

Správce by také měl mít dohody se svými zpracovateli, kteří sami mají povinnost ohlásit správci případ porušení (viz dále).

Je na odpovědnosti správců a zpracovatelů zavést vhodná opatření umožňující předcházet případům porušení, reagovat na ně a řešit je a zde je několik praktických kroků, které by měli v každém případě učinit.

- Informace o všech s bezpečností souvisejících událostech by měly být směrovány na odpovědnou osobu nebo osoby pověřené řešením incidentů, zjišťováním výskytu porušení a posuzováním rizika.
- Mělo by být posouzeno riziko, které má porušení za následek pro jednotlivce (pravděpodobnost nulového rizika, rizika nebo vysokého rizika), a měly by o tom být informovány příslušné útvary v organizaci.
- Ohlášení případu dozorovému úřadu a případně informování dotčených jednotlivců by mělo být provedeno, je-li vyžadováno.
- Správce by současně měl podniknout kroky ke zvládnutí případu porušení a odstranění jeho následků.

Mělo by také být jasné, že správce má povinnost jednat na základě prvního upozornění a zjistit, zda k porušení skutečně došlo či ne. V tomto krátkém časovém úseku, ještě než správce případně udělá ohlášení, lze provést určité šetření, shromáždit důkazy a vyhodnotit riziko. Pokud ovšem správce s dostatečnou jistotou zjistil, že k porušení došlo a jsou-li naplněny podmínky podle článku 33, odst. 1, pak musí bezodkladně provést ohlášení dozorovému úřadu a, pokud je to proveditelné, do 72 hodin. Neučiní-li tak správce včas a bude zřejmé, že k porušení došlo, může to být považováno za nesplnění ohlašovací povinnosti podle článku 33.

Článek 32 jasně stanovuje, že správce i zpracovatel by měli přijmout vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající osobních údajů: schopnost odhalit a řešit porušení a včas o něm informovat by měla být vnímána jako základní prvek těchto opatření.

3. Povinnosti zpracovatele

Správce nese celkovou odpovědnost za ochranu osobních údajů, ale zpracovatel hraje důležitou roli, když správci umožňuje být v souladu se svými povinnostmi; což se týká také ohlašování případů porušení. V článku 28, odst. 3 rovněž stojí, že zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem. Článek 28, odst. 3, písm. f) říká, 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“.

Článek 33, odst. 2 říká jasně, že pokud správce používá zpracovatele a tento zpracovatel zjistí porušení zabezpečení osobních údajů, jež pro správce zpracovává, musí to správci ohlásit „bez zbytečného odkladu“. Správce používá zpracovatele k naplnění svých účelů; proto, v zásadě, by mělo platit, že správce se „dozvěděl“ o porušení ve chvíli, kdy se o něm dozvěděl zpracovatel. Povinnost zpracovatele informovat správce umožňuje správci, aby případ řešil a určil, zda bude nutné jej ohlásit dozorovému úřadu v souladu s článkem 33, odst. 1 a zda informovat dotčené jednotlivce podle článku 34, odst.1.

[17] Je dobré vědět, že logová data usnadňují kontrolovatelnost, např. informace o ukládání, modifikování nebo vymazávání dat může také být považována za osobní údaje týkající se osoby, která zahájila danou operaci zpracování.

Obecné nařízení nestanovuje explicitní časový limit, do kdy zpracovatel musí upozornit správce, pouze říká, že tak musí učinit „bez zbytečného odkladu“. WP29 proto doporučuje okamžité ohlášení zpracovatelem správci s tím, že další informace o porušení budou sdělovány postupně, jak budou k dispozici. To je důležité z hlediska pomoci správci splnit ohlašovací požadavky vůči dozorovému úřadu během 72 hodin.

Poskytuje-li zpracovatel služby více správcům, kteří všichni byli postiženi tím samým incidentem, musí zpracovatel ohlásit podrobnosti o tomto incidentu všem správcům.

Zpracovatel by mohl provést ohlášení jménem správce, pokud tento mu dal řádné oprávnění, které je součástí smluvního ujednání mezi správcem a zpracovatelem. Ohlášení musí být učiněno v souladu s články 33 a 34. Je však důležité vzít na vědomí, že právní odpovědnost provést ohlášení zůstává na správci.

Jak je vysvětleno výše, správci mají ve svých smlouvách se zpracovateli specifikovat, jak budou splněny požadavky vyjmenované v článku 33, odst. 2.

B. Poskytnutí informací dozorovému úřadu

1. Informace, které mají být poskytnuty

Ohlašuje-li správce případ porušení dozorovému úřadu, pak podle článku 33, odst. 3 musí 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.“

Obecné nařízení nedefinuje kategorie subjektů údajů nebo záznamů osobních údajů. Ovšem WP29 navrhuje, aby se kategorie subjektů údajů vztahovaly k různým typům jednotlivců, jejichž osobní údaje byly porušením dotčeny: v závislosti na používaných deskriptorech by to mohly být, mimo jiné, děti a další zranitelné skupiny, lidé s postižením, zaměstnanci nebo zákazníci. Obdobně, kategorie záznamů osobních údajů mohou odkazovat na různé typy záznamů, které správce případně zpracovává, jako jsou zdravotní data, školní záznamy, informace o sociální péči, finanční údaje, čísla bankovních účtů, čísla pasů atd.

Recitál 85 objasňuje, že jedním z účelů ohlašování je omezení újmy způsobené fyzickým osobám. Proto pokud určité typy subjektů údajů nebo typy osobních údajů indikují riziko konkrétní škody v důsledku porušení (např. krádež identity, podvod, finanční ztráta, ohrožení profesionálního tajemství), pak má význam, aby v ohlášení byly tyto kategorie uvedeny. V tomto smyslu je tu návaznost na požadavek popsat pravděpodobné důsledky porušení zabezpečení.

Pro včasné ohlášení porušení by neměla být na překážku neexistence přesných informací (např. přesný počet dotčených subjektů údajů). Obecné nařízení umožňuje počet dotčených jednotlivců a počet záznamů osobních údajů odhadnout. Pozornost by měla být soustředěna na nežádoucí účinky porušení než na poskytnutí přesných čísel. Takže pokud je jasné, že došlo k porušení, ale není ještě znám jeho rozsah, bezpečnou cestou, jak splnit ohlašovací povinnost, je ohlašovat postupně (viz dále).

Článek 33, odst. 3 říká, že správce „musí přinejmenším“ v ohlášení poskytnout vyjmenované informace, takže se může, je-li to nutné, rozhodnout podat i další podrobnosti. U různých typů porušení (důvěrnost, integrita nebo dostupnost) může vzniknout požadavek poskytnout další informace pro úplné vysvětlení okolností každého případu.

Příklad

V rámci ohlášení dozorovému úřadu může správce dojít k názoru, že bude užitečné uvést jméno svého zpracovatele, je-li u kořene příčiny porušení, zejména pokud to vedlo k incidentu dopadajícímu na záznamy osobních údajů mnoha dalších správců používajících toho samého zpracovatele.

Dozorový úřad si může v každém případě vyžádat další podrobnosti v rámci svého šetření.

2. Postupné ohlašování

V závislosti na povaze porušení může být nutné další šetření ze strany správce, aby zjistil všechny podstatné skutečnosti ohledně incidentu. Článek 33, odst. 4 proto říká:

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

Znamená to, že Obecné nařízení připouští, že správci nebudou pokaždé mít všechny nezbytné informace ohledně porušení během 72 hodin od zjištění, jelikož v počáteční fázi nemusí vždy být k dispozici plné a srozumitelné informace o incidentu. Proto dovoluje postupné ohlašování. Bude to spíše případ složitějších porušení, jako jsou některé incidenty týkající se kybernetické bezpečnosti, kde, například, může být nutné hloubkové forenzní šetření k úplnému zjištění povahy případu a rozsahu, v jakém jsou osobní data ohrožena. V mnoha případech bude tedy správce muset provést další podrobnější šetření a přijít následně s dodatečnými informacemi v pozdějším čase. To je přípustné za předpokladu, že správce zpoždění zdůvodní v souladu s článkem 33, odst. 1. WP29 doporučuje, aby správce při prvním ohlašování dozorovému úřadu uvedl, zda ještě poskytne více informací později. Dozorový úřad by měl odsouhlasit, jak a kdy budou dodatečné informace poskytnuty.

Záměrem požadavku ohlašování je povzbudit správce k rychlé reakci na porušení, jeho zvládnutí a, pokud možno, obnovu ohrožených osobních údajů, jakožto i vyžádání příslušné rady od dozorového úřadu. Ohlášení dozorovému úřadu během prvních 72 hodin může pro správce znamenat jistotu, že rozhodnutí oznámit nebo neoznámit případ jednotlivcům, je správné.

Účelem ohlašování dozorovému úřadu však není jen získat pokyny, zda uvědomit dotčené jednotlivce. V některých případech bude zřejmé, že, vzhledem k povaze porušení a závažnosti rizika, bude správce muset případ bezodkladně oznámit dotčeným jednotlivcům. Například, hrozí-li bezprostředně krádež totožnosti nebo jsou-li na internetu zpřístupněny zvláštní kategorie osobních údajů[18], pak by správce měl jednat bez zbytečného odkladu, aby porušení zvládnul a informoval dotčené jednotlivce (viz oddíl IV). Za mimořádných okolností by se tak mělo stát dokonce ještě před ohlášením dozorovému úřadu. Obecněji řečeno, ohlášení dozorovému úřadu nesmí sloužit jako výmluva pro neoznámení případu porušení subjektu údajů, je-li to vyžadováno.

Mělo by být také jasné, že po prvotním ohlášení, pokud následné šetření odhalí odpovídající důkaz, správce může dozorový úřad informovat, že bezpečnostní incident zvládnul a k žádnému porušení ve skutečnosti nedošlo. Tato informace pak může být přiložena k informaci dozorovému úřadu již předané a může zadokumentovat, že incident nebyl porušením. Ohlášení incidentu, u kterého nakonec vyjde najevo, že nebyl porušením zabezpečení, nebude pokutováno.

Příklad

Správce ohlásí dozorovému úřadu během 72 hodin od zjištění případu ztrátu CD obsahujícího osobní údaje některých jeho zákazníků. Toto CD je později nalezeno jako nesprávně založené uvnitř správcových prostor a jeho funkčnost je obnovena. Správce o tom informuje dozorový úřad a požádá o aktualizaci ohlášení.

Mělo by být řečeno, že postupný přístup k ohlašování už je zakotven v existujících povinnostech podle Směrnice 2002/58/ES, Nařízení 611/2013 a v dalších případech samoohlašování.

3. Opožděné ohlášení

Článek 33, odst. 1 vyjasňuje, že pokud ohlášení dozorovému úřadu není učiněno do 72 hodin, mělo by to být zdůvodněno. Toto ustanovení, spolu s konceptem postupného ohlašování, připouští, že správce nemusí vždy být schopen ohlásit porušení během stanovené lhůty a opožděné ohlášení může být přípustné.

Takový scénář nastane, třeba když správce čelí několikerým podobným porušením důvěrnosti v krátkém časovém období, která stejným způsobem postihují velké počty subjektů údajů. Správce se může dozvědět o porušení, a zatímco zahajuje šetření, ještě před ohlášením, odhalí další podobné případy mající různé příčiny. Podle okolností

[18] Viz článek 9.

může správci nějaký čas trvat, než zjistí rozsah těchto porušení a než aby ohlašoval každý případ jednotlivě, správce raději připraví smysluplné ohlášení reprezentující několik velmi podobných porušení s potenciálně různými příčinami. Tento přístup může zpozdit ohlášení dozorovému úřadu za hranici 72 hodin od okamžiku, kdy se správce poprvé o těchto případech dozvěděl.

Přísně vzato je každé jednotlivé porušení hlásitelný incident. Aby se však předešlo přílišné zátěži, může správce podat „hromadné" ohlášení pokrývající všechna tato porušení, za podmínky, že se týkají stejného typu osobních údajů, jejichž zabezpečení bylo porušeno stejným způsobem během poměrně krátké doby. Dojde-li k sérii porušení postihujících různé druhy osobních údajů a stalo-li se tak různými způsoby, pak by ohlášení mělo probíhat normální cestou, tedy každý případ by měl být ohlášen v souladu s článkem 33.

Obecné nařízení sice do jisté míry povoluje opožděná hlášení, nemělo by to však být považováno za běžnou praxi. Stojí za to poukázat na to, že hromadná ohlášení lze také učinit pro početná a podobná porušení hlášená během 72 hodin.

C. Porušení postihující jednotlivce ve více než jednom členském státě

U přeshraničního zpracování[19] osobních údajů se porušení může týkat subjektů údajů ve více než jednom členském státě. Článek 33, odst. 1 říká, že pokud dojde k porušení, měl by to správce ohlásit dozorovému úřadu příslušnému podle článku 55 Obecného nařízení[20]. Článek 55, odst. 1 praví:

> „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."

Článek 56, odst. 1 však 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."

Článek 56, odst. 6 dále říká:

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

To znamená, že vždy, když porušení postihne osobní údaje jednotlivců z více než jednoho členského státu a je vyžadováno ohlášení, bude muset správce uvědomit vedoucí dozorový úřad[21]. Proto musí správce při sestavování plánu reakce na porušení vypracovat posouzení ohledně stanovení, který dozorový úřad bude pro něho vedoucí a tedy příslušný pro ohlášení[22]. Správci to umožní rychle reagovat na porušení a splnit povinnosti vyplývající z článku 33. Pokud bude správce mít jakékoliv pochyby ohledně stanovení vedoucího úřadu, musí alespoň uvědomit dozorový úřad příslušný podle místa, kde k porušení došlo. Správce se může aktivně rozhodnout ohlásit incident dozorovému úřadu, který není vedoucím, například, je-li správci známo, že jednotlivci v jiných členských státech byli porušením dotčeni. Jestliže se však správce rozhodne uvědomit pouze vedoucí dozorový úřad, doporučuje se, aby v náležitém případě uvedl, zda se porušení dotýká provozoven sídlících v jiných členských státech, a ve kterých členských státech je pravděpodobné, že budou porušením dotčeny subjekty údajů.

D. Podmínky, za kterých ohlášení není vyžadováno

Článek 33, odst. 1 vysvětluje, že případy, kdy „je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob", nevyžadují ohlášení dozorovému úřadu. Jako příklad může posloužit situace, kdy osobní údaje byly již veřejně dostupné a jejich zpřístupnění tak nepředstavuje pravděpodobné riziko pro jednotlivce. Kontrastuje to se stávajícími požadavky ohledně ohlašování porušení platné pro poskytovatele

[19] Viz článek 4, odst. 23
[20] Viz recitál 122.
[21] Viz Pokyny WP29 pro určení vedoucího dozorového úřadu správce nebo zpracovatele, dostupné na http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[22] Seznam kontaktů na všechny evropské národní dozorové úřady lze najít na: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

veřejně dostupných služeb elektronických komunikací podle Směrnice 2009/136/ES, která stanoví, že veškerá relevantní porušení musí být ohlášena příslušnému úřadu.

Ve Stanovisku 03/2014 k ohlašování porušení zabezpečení[23] vysvětluje WP29, že porušení důvěrnosti osobních údajů zašifrovaných moderním algoritmem, je pořád porušením zabezpečení a musí jako takové být ohlášeno. Pokud ovšem utajení klíče trvá – tj. klíč nebyl při žádném bezpečnostním incidentu prozrazen a byl vygenerován tak, že nemůže být odhalen dostupnými technickými prostředky, žádnou k přístupu oprávněnou osobou – pak data jsou v zásadě nečitelná. Je tak nepravděpodobné, že by se nepříznivě dotknul jednotlivců a proto informování těchto jednotlivců není vyžadováno[24]. Avšak dokonce i v případě šifrovaných dat může mít jejich ztráta nebo pozměnění neblahé důsledky pro subjekty údajů, pokud správce nemá odpovídající zálohy. V takovém případě by oznámení subjektům údajů bylo vyžadováno, byť data samotná byla odpovídajícím způsobem zašifrována.

WP29 také vysvětlila, že podobně by to platilo, pokud by na osobní údaje, jako jsou hesla, bylo bezpečně uplatněno hašování nebo kryptografická sůl, hašovací hodnota by byla vypočítána moderní kryptografickou hašovací funkcí s použitím klíče, přičemž tento klíč by nebyl prozrazen v důsledku nějakého porušení zabezpečení a klíč použitý k hašování dat by byl vytvořen způsobem, který neumožňuje jeho zjištění pomocí dostupných technologických prostředků žádnou osobou, která nemá přístupové oprávnění.

Proto pokud osobní údaje byly v zásadě učiněny nesrozumitelnými pro neoprávněné strany a jsou kopií nebo existuje záloha, pak porušení důvěrnosti řádně zašifrovaných osobních údajů nemusí být ohlášeno dozorovému úřadu. A to vzhledem k tomu, že je nepravděpodobné, že takové porušení by mohlo mít za následek riziko pro práva a svobody jednotlivců. Znamená to, že nebude ani potřeba provést oznámení jednotlivci, jelikož pravděpodobně nehrozí žádné velké riziko. Mělo by však být pamatováno na to, že, zatímco ohlášení nemusí zpočátku být vyžadováno, neexistuje-li pravděpodobnost rizika pro práva a svobody jednotlivců, může se tato situace časem změnit a riziko bude třeba přehodnotit. Například zjistí-li se následně, že klíč byl prozrazen nebo bude odhaleno zranitelné místo v šifrovacím softwaru, pak ohlášení přece jen může být vyžadováno.

Je také potřeba říci, že pokud dojde k porušení u zašifrovaných dat, která nejsou zálohována, pak se bude jednat o narušení dostupnosti, které by mohlo představovat riziko pro jednotlivce, a proto může být vyžadováno ohlášení. Podobně, pokud dojde k porušení zahrnující ztrátu zašifrovaných údajů, byť při existenci zálohy, může pořád jít o hlásitelný případ, podle toho, jak dlouho bude trvat obnova údajů ze záložního souboru a jaký dopad bude nedostupnost mít na jednotlivce. Jak stanoví článek 32, odst. 1, písm. c), významným bezpečnostním faktorem je „schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů“.

Příklad

Příkladem porušení, které nevyžaduje ohlášení dozorovému úřadu, je ztráta bezpečně zašifrovaného mobilního zařízení používaného správcem a jeho zaměstnanci. Za podmínky, že šifrovací klíč zůstal v bezpečném držení správce a nejde o jedinou kopii osobních údajů, jsou osobní údaje pro útočníka nedostupné. Znamená to, že případ porušení pravděpodobně nevyústí v riziko pro práva a svobody dotčených subjektů údajů. Vyjde-li později najevo, že šifrovací klíč byl prozrazen nebo že šifrovací software nebo algoritmus je zranitelný, pak se úroveň rizika pro práva a svobody fyzických osob změní a ohlášení může být vyžadováno.

K porušení článku 33 však dojde, pokud správce neprovede ohlášení dozorovému úřadu v situaci, kdy data ve skutečnosti nebyla bezpečně zašifrována. Proto by správci při výběru šifrovacího softwaru měli pečlivě vážit kvalitu a správnou implementaci nabízeného šifrování, chápat, jakou úroveň ochrany skutečně nabízí a zda odpovídá existujícím rizikům. Správci by se také měli dobře obeznámit s konkrétními charakteristikami fungování šifrovacího produktu. Zařízení může například být zašifrováno ve chvíli, kdy je vypnuto, ale nikoliv v režimu stand-by. Některé výrobky používající šifrování mají „přednastavené klíče“, které musí každý zákazník změnit, aby byly účinné. Šifrování může také být bezpečnostními experty bráno za aktuálně odpovídající, ale během několika let může zastarat, takže je pak sporné, zda budou data tímto produktem dostatečně zašifrovaná a na odpovídající úrovni chráněna.

III. Článek 34 – Oznamování subjektu údajů

A. Informování jednotlivců

[23] WP29, Stanovisko 03/2014 k ohlašování porušení zabezpečení, http://ec.europa.eu/iustice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[24] Viz také článek 4, odst.1 a odst. 2 v Nařízení 611/2013.

V určitých případech musí správce, kromě ohlášení dozorovému úřadu, případ porušení oznámit také dotčeným jednotlivcům.

Článek 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 dozorovému úřadu je povinné, pokud je pravděpodobné, že určitý případ porušení bude mít za následek riziko pro jednotlivce. A navíc, pokud existuje pravděpodobnost vysokého rizika pro práva a svobody jednotlivců v důsledku porušení, musí pak být informováni i oni. Spouštěcí hranice pro oznámení případu jednotlivcům je tedy vyšší, než u ohlašování dozorovému úřadu a proto ne u všech porušení bude vyžadováno oznámení jednotlivcům, aby byli ušetřeni zbytečné informační zátěže.

Obecné nařízení stanoví, že oznámení o porušení jednotlivcům by mělo být učiněno „bez zbytečného odkladu", tj. co nejdříve. Hlavním účelem oznamování jednotlivcům je poskytnutí konkrétní informace o krocích, které by měli učinit pro vlastní ochranu[25]. Jak je řečeno výše, v závislosti na povaze porušení a riziku, pomůže včasné oznámení jednotlivcům, aby podnikli kroky k vlastní ochraně před všemi negativními důsledky porušení.

Příloha B těchto vodítek uvádí seznam, ne ovšem vyčerpávající, příkladů, kdy je pravděpodobné, že porušení může vést k vysokému riziku pro jednotlivce a následně k případům, kdy správce musí oznámit porušení dotčeným osobám.

B. Informace, které mají být poskytnuty

Ohledně oznámení jednotlivcům článek 34, odst. 2 upřesňuje, že:

> „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 článku 33 odst. 3 písm. b), c) a d)."

Podle tohoto ustanovení by správce měl poskytnout alespoň následující informace:

- popis povahy porušení;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiné kontaktní místo;
- popis pravděpodobných důsledků porušení; a
- popis opatření přijatých nebo navržených správcem pro řešení případu, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

V rámci takových opatření k řešení případu porušení a ke zmírnění jeho možných nepříznivých dopadů by například správce měl, poté co ohlásil porušení příslušnému dozorovému úřadu, prohlásit, že obdržel radu ohledně zvládnutí případu a zmírnění jeho dopadu. Správce by také ve vhodných případech měl jednotlivcům poskytnout konkrétní radu, jak se chránit před možnými nepříznivými důsledky porušení, jako je resetování hesla v případě, kdy byly prozrazeny jejich přístupové údaje. Správce se ovšem může rozhodnout podat další informace nad rámec toho, co je požadováno.

C. Kontaktování jednotlivců

Daný případ porušení může v zásadě být dotčeným subjektům údajů oznámen přímo, ledaže by to vyžadovalo neúměrné úsilí. V takovém případě lze namísto toho učinit veřejné oznámení nebo podobné opatření, kdy subjekty údajů budou informovány stejně účinným způsobem (Článek 34, odst. 3, písm. c).

K oznamování porušení subjektům údajů by měly být užívány samostatné zprávy a neměly by je doprovázet další informace, jako pravidelné aktualizace, newslettery nebo standardní sdělení. Oznámení porušení tak bude jasné a transparentní.

Příklady způsobů transparentní komunikace zahrnují přímé textování (např. e-mail, SMS, přímá zpráva), výrazné bannery nebo oznámení na webových stránkách, komunikace poštou a nápadné reklamy v tištěných médiích.

[25] Viz také recitál 86.

Oznámení skryté v tiskové zprávě nebo na korporátním blogu nepředstavují účinné prostředky oznámení případu jednotlivci. WP29 správcům doporučuje, aby vybírali prostředky maximalizující šanci správného přenosu informací ke všem subjektům údajů. Podle okolností může správce, namísto jednoho oznamovacího kanálu, použít několik způsobů komunikace.

Správci by se také případně měli postarat, aby oznámení bylo k dispozici ve vhodných alternativních formátech a relevantních jazycích, aby jednotlivci poskytované informaci rozuměli. Kupříkladu oznámení v rodném jazyce příjemce pomůže zajistit porozumění povaze případu a krokům, které mohou učinit pro svou ochranu.

Správci mohou nejlépe určit odpovídající komunikační kanál vůči jednotlivcům cestou hojné interakce se svými zákazníky. Správce by si však měl dávat pozor, aby nepoužil kanál dotčený porušením, jelikož by mohl být využit útočníkem vydávajícím se za správce.

Recitál 86 vysvětluje:

> „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 tedy mohli kontaktovat a konzultovat dozorový úřad ne jenom kvůli radě ohledně informování subjektů údajů o porušení v souladu s článkem 34, ale také ve věci náležitosti zpráv zasílaných jednotlivcům a nejvhodnějších způsobů jejich kontaktování.

D. Podmínky, za kterých ohlášení není vyžadováno

Článek 34, odst. 3 stanoví tři podmínky, při jejichž splnění není vyžadováno oznámit jednotlivcům případ porušení. Jedná se o tyto podmínky:

- správce zavedl náležitá technická a organizační ochranná opatření ještě před případem porušení, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup. Sem by například mohlo patřit použití nejmodernějšího způsobu šifrování osobních údajů.
- ihned po incidentu správce zajistil, že vysoké riziko pro práva a svobody jednotlivců se již pravděpodobně neprojeví. Například, podle okolností případu, správce stanovil a podniknul kroky vůči tomu, kdo se dostal k osobním údajům dříve, než s nimi mohl něco udělat. Patřičnou pozornost je potřeba věnovat možným důsledkům jakéhokoli porušení důvěrnosti, opět v závislosti na povaze dotčených dat.
- kontaktovat jednotlivce by vyžadovalo neúměrné úsilí[26], třeba když jejich kontaktní údaje byly ztraceny v důsledku porušení nebo nejsou zprvu známy. Například, úložiště statistické kanceláře přeteklo a dokumenty obsahující osobní údaje byly skladovány jen v papírové podobě. Správce v tomto případě musí zveřejnit oznámení nebo učinit podobné opatření informující jednotlivce stejně účinným způsobem. V případě neúměrného úsilí lze uvažovat o technických opatřeních k poskytnutí informací o porušení na vyžádání, což by se mohlo osvědčit u těch osob, které mohly být incidentem dotčeny, avšak správce je nemohl jiným způsobem kontaktovat.

V souladu se zásadou odpovědnosti by správci měli být schopni doložit dozorovému úřadu, že dodržují jednu nebo více z těchto podmínek[27]. Nemělo by se zapomínat, že ohlášení nemusí zpočátku být vyžadováno, pokud neexistuje riziko pro práva a svobody fyzických osob, což se ale během času může změnit a riziko pak bude třeba přehodnotit.

Pro případ, kdy se správce rozhodne porušení jednotlivci neoznámit, stanovuje článek 34, odst. 4, že dozorový úřad to přece jen může požadovat, dojde-li k názoru, že porušení by mohlo mít za následek vysoké riziko pro jednotlivce. Případně může usoudit, že podmínky článku 34, odst. 3 byly splněny a oznámení jednotlivcům nevyžadovat. Pokud dozorový úřad dozná, že rozhodnutí neinformovat subjekty údajů není dostatečně podloženo, může zvážit využití svých dostupných pravomocí a sankcí.

IV. **Posuzování rizika a vysokého rizika**

[26] Viz připravované Pokyny WP29 k transparentnosti, kde téma neúměrného úsilí bude pojednáno.
[27] Viz článek 5, odst. 2

A. Riziko jako spouštěč ohlášení

Ačkoliv Obecné nařízení zavádí ohlašovací povinnost v případě porušení, nejedná se o požadavek, který je nutno splnit za všech okolností:

- ohlašovací povinnost dozorovému úřadu je spuštěna, jen když je pravděpodobné, že porušení bude mít za následek riziko pro práva a svobody jednotlivců.
- oznamovací povinnost vůči jednotlivci je spuštěna, jen když je pravděpodobné, že porušení bude mít za následek vysoké riziko pro jeho práva a svobody.

Pro správce to znamená, že ihned poté, co se dozví o porušení, je nezbytně důležité, aby se snažil nejenom případ zvládnout, ale také aby posoudil, jaké riziko by incident mohl mít za následek. Ze dvou významných důvodů: předně, povědomí o pravděpodobnosti a možné závažnosti dopadu na jednotlivce pomůže správci přijmout účinné kroky k vypořádání se s porušením; a za druhé, pomůže to při stanovení, jestli je ohlášení dozorovému úřadu nutné a zda je také nutné učinit oznámení dotčeným jednotlivcům.

Jak bylo vysvětleno výše, klíčovým spouštěčem pro ohlášení porušení je pravděpodobnost rizika pro práva a svobody jednotlivců a hlavním spouštěčem pro oznámení případu subjektům údajů je pravděpodobnost *vysokého* rizika pro práva a svobody jednotlivců. Takové riziko existuje v případě, že porušení může u dotčeného jednotlivce vést k tělesné, materiální nebo nemateriální škodě. Příklady takové škody jsou diskriminace, krádež totožnosti nebo podvod, peněžní ztráta a poškození pověsti. Týká-li se porušení i osobních údajů vypovídajících o rasovém nebo etnickém původu, politickém názoru, náboženském nebo filozofickém přesvědčení, členství v odborech, či zahrnuje genetická data nebo údaje týkající se zdraví nebo pohlavního života, rozsudků v trestních věcech a trestných činů, měl by výskyt takové škody být považován za pravděpodobný[28].

B. Faktory připadající v úvahu při posuzování rizika

Recitály 75 a 76 Obecného nařízení říkají, že obecně při posuzování rizika by měla být v úvahu vzata jeho pravděpodobnost a závažnost ve vztahu k právům a svobodám subjektů údajů. Dále říká, že riziko by mělo být hodnoceno na základě objektivního posouzení.

Je třeba si povšimnout, že hodnocení rizika vůči lidským právům a svobodám, které je následkem porušení zabezpečení, je zaměřeno jinak, než v případě posouzení vlivu na ochranu osobních údajů[29]. Posouzení vlivu bere v úvahu jak rizika vyplývající z plánovaného zpracování dat, tak rizika v případě porušení zabezpečení. Při úvahách o potenciálním porušení se obecně hledí na pravděpodobnost jeho výskytu a škody, která může vyvstat pro subjekt údajů; jinými slovy, jde o posouzení hypotetické události. Když už k porušení dojde, jedná se o hotovou věc, přičemž pozornost se plně soustřeďuje na výsledné riziko vlivu incidentu na jednotlivce.

Příklad

Posouzení vlivu říká, že navrhované použití určitého bezpečnostního softwaru k ochraně osobních údajů je vhodným opatřením pro zajištění úrovně zabezpečení, která odpovídá riziku, jež by jinak zpracování pro jednotlivce představovalo. Pokud by se však později objevilo nějaké zranitelné místo, změnila by se vhodnost softwaru k zamezení rizik pro chráněné osobní údaje a bylo by pak potřeba znovu přehodnotit část stávajícího posouzení vlivu.

Někdo zneužije zranitelnosti produktu a dojde k incidentu. Správce by měl posoudit konkrétní okolnosti porušení, jaká data byla zasažena a možnou úroveň dopadu na jednotlivce a dále také, s jakou pravděpodobností se toto riziko může projevit.

[28] Viz recitál 75 a recitál 85.
[29] Viz Pokyny WP29 k posouzení vlivu: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Správce tedy při posuzování rizika pro jednotlivce následkem porušení vezme v úvahu konkrétní okolnosti případu včetně jeho závažnosti a možného dopadu. WP29 proto doporučuje vzít při posuzování v úvahu následující kritéria[30]:

- Typ porušení

Typ nastalého porušení může ovlivnit úroveň rizika pro jednotlivce. Například porušení důvěrnosti, kdy došlo ke zpřístupnění lékařských informací neoprávněným osobám, může pro jednotlivce mít jiné důsledky, než by mělo porušení spočívající v jejich ztrátě, kdy data už nejsou k dispozici vůbec.

- Povaha, citlivost a objem osobních údajů

Při posuzování rizika je klíčovým faktorem pochopitelně druh a citlivost osobních údajů, které byly porušením ohroženy. Obvykle platí, že čím citlivější data, tím vyšší riziko pro dotčené lidi, avšak v úvahu by bylo dobré vzít také ostatní osobní údaje, které už o subjektu údajů jsou dostupné. Například je nepravděpodobné, že za běžných okolností může zpřístupnění jména a adresy jednotlivce způsobit podstatnou škodu. Pokud však dojde ke zpřístupnění jména a adresy adoptivního rodiče biologickému rodiči, mohou být následky pro adoptivního rodiče i dítě velmi závažné.

Incidenty zahrnující zdravotní data, dokumenty totožnosti nebo finanční data, jako informace z kreditních karet, mohou všechny samy o sobě způsobit nějakou újmu, ale dohromady by mohly být zneužity ke krádeži identity. Kombinace osobních údajů bývá více citlivá než jednotlivá datová položka.

Některé druhy osobních údajů mohou zpočátku vypadat docela nevinně, přesto však by mělo být pečlivě zváženo, co tato data mohou o dotyčném jednotlivci vypovědět. Seznam zákazníků přijímajících pravidelné dodávky nemusí být nijak zvlášť citlivý, ale ta samá data o zákaznících, kteří požádali o přerušení dodávek po dobu dovolené, už by byla užitečnou informací pro zloděje.

Obdobně, malé množství vysoce citlivých osobních údajů může mít značný dopad na jednotlivce a velký rozsah podrobností může o jednotlivci odhalit širší škálu informací. Rovněž porušení postihující velké objemy osobních dat může mít vliv na odpovídající velký počet jednotlivců.

- Snadnost identifikace jednotlivců

Zvážit je třeba jeden důležitý faktor, a sice, jak snadné bude pro někoho s přístupem k napadeným osobním údajům identifikovat konkrétního jedince nebo propojit tyto údaje s dalšími informacemi za účelem jeho ztotožnění. Podle okolností by identifikace jednotlivce mohla být možná přímo z narušených osobních dat, bez nutnosti zvláštního zkoumání nebo by přiřazení osobních údajů ke konkrétnímu jedinci mohlo být značně náročné, ale přesto by to však za jistých podmínek bylo možné. Identifikace na základě uniklých dat může být přímo nebo nepřímo možná, může však záležet na konkrétních souvislostech případu a na veřejné dostupnosti souvisejících osobních dat. Může to platit zejména pro případy porušení důvěrnosti a dostupnosti. Jak bylo řečeno výše, osobní údaje chráněné šifrováním na náležité úrovni budou nesrozumitelné pro nepovolané osoby bez dešifrovacího klíče. Pseudonymizace, což je proces skrytí identity dat přiřazením kódového odkazu nebo pseudonymu k určitému záznamu, aby bylo možno data přiřadit k určitému jednotlivci, aniž by tento byl identifikován, může snížit pravděpodobnost odhalení totožnosti osoby případě porušení.

- Závažnost důsledků pro jednotlivce

V závislosti na povaze porušení dotčených osobních údajů, například u zvláštní kategorie dat, může být potenciální škoda pro jednotlivce zvláště závažná, zejména pokud by porušení mohlo vést ke krádeži totožnosti nebo podvodu, tělesné újmě, psychické nepohodě, potupě nebo poškození pověsti. Dotýká-li se porušení osobních údajů zranitelných jednotlivců, může to pro ně představovat vyšší riziko újmy.

[30] Článek 3.2 Nařízení 611/2013 podává návod ohledně faktorů, které by měly být zváženy v souvislosti s ohlašováním porušení v oblasti služeb elektronických komunikací, jenž může být užitečný i v kontextu ohlašování podle Obecného nařízení.

Vědomost správce o tom, že osobní údaje jsou v rukách lidí s neznámými nebo snad zlovolnými záměry, může mít vliv na úroveň potenciálního rizika. Může dojít k porušení důvěrnosti, přičemž budou osobní údaje omylem odkryty třetí straně podle definice článku 4, odst. 10 nebo jinému příjemci. Může to například nastat, pokud budou osobní údaje nedopatřením odeslány nesprávnému oddělení nebo organizaci nebo běžně používanému dodavateli. Správce může příjemce požádat o navrácení nebo bezpečné zničení obdržených dat. V obou případech, vzhledem k trvalému vztahu, který s nimi správce má a k povědomí o jejich postupech, minulosti a dalších podstatných skutečnostech, lze příjemce považovat za „důvěryhodného". Jinak řečeno, správce může mít takovou důvěru v příjemce, že důvodně očekává, že nebude číst nebo přistupovat k omylem zaslaným datům a vyhoví žádosti o jejich navrácení. Dokonce, i když příjemce do dat nahlédne, může se správce stále spoléhat, že s nimi dále nic nepodnikne a okamžitě je vrátí správci a bude s ním spolupracovat při jejich obnově. Takové případy mohou být chápány jako posouzení rizika provedené správcem v návaznosti na porušení – skutečnost, že příjemce má důvěru, může eliminovat závažnost důsledků případu, však neznamená , že k porušení nedošlo. A může to také vynulovat pravděpodobnost rizika pro jednotlivce, čímž nebude vyžadováno ohlášení dozorovému úřadu ani oznámení dotčeným jednotlivcům. I zde to však bude platit případ od případu. Správce ovšem beztak bude muset incident zaznamenat v rámci povinnosti vést záznamy o případech porušení (viz oddíl VI).

Zvážit by bylo potřeba i trvání důsledků pro jednotlivce, kdy v případě dlouhodobých účinků může být dopad větší.

- Zvláštní charakteristiky jednotlivce

Porušení může postihnout osobní údaje týkající se dětí nebo dalších zranitelných jednotlivců, kteří tak mohou být vystaveni vyššímu riziku nebezpečí. Mohou existovat i další faktory související s jednotlivcem, které mohou ovlivnit úroveň dopadu porušení.

- Počet dotčených jednotlivců

Porušení může postihnout jen jednoho nebo několik jednotlivců anebo také několik tisíc, ne-li více. Obecně řečeno, čím vyšší počet dotčených jednotlivců, tím větší dopad porušení může mít. Porušení však může mít závažný dopad i jen na jednoho člověka, podle povahy ohrožených osobních údajů a souvislostí, za kterých se tak stalo.

- Zvláštní charakteristiky správce

Povaha a role správce a jeho činnosti mohou ovlivňovat výši rizika, které jednotlivcům hrozí následkem porušení. Například zpracování zvláštních kategorií osobních údajů ve zdravotnickém zařízení bude ve srovnání s distribučním seznamem nějakých novin představovat větší ohrožení pro jednotlivce v případě porušení zabezpečení jeho osobních údajů.

- Obecné skutečnosti

Proto by při posuzování pravděpodobného rizika následkem porušení měl správce vzít v potaz kombinaci závažnosti možného dopadu do práv a svobod jednotlivců a pravděpodobnost, že se tak vůbec stane. Je jasné, že jsou-li důsledky porušení závažnější, je i riziko vyšší a podobně, kde je pravděpodobnost události vyšší, je také riziko zvýšené. V případě pochybností by správce měl upřednostnit opatrnost a případ ohlásit. V příloze B je uvedeno několik užitečných příkladů různých typů porušení nesoucích s sebou riziko nebo vysoké riziko pro jednotlivce.

Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) vypracovala doporučení pro metodiku posuzování závažnosti porušení, které správci a zpracovatelé mohou shledat užitečným při zpracování svého plánu, jak reagovat na incidenty a zvládat je[31].

V. Odpovědnost a vedení záznamů

A. Dokumentace případů porušení

Ať už porušení je nebo není třeba ohlásit dozorovému úřadu, musí správce vést dokumentaci o veškerých případech, jak vysvětluje článek 33, odst. 5:

[31] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https ://www. enisa. europa.eu/publications/dbn-severity

„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."

Je zde vazba na zásadu odpovědnosti podle Obecného nařízení, článek 5, odst. 2. Správci jsou tak pobízeni k založení vnitřního registru případů porušení, bez ohledu na to, zda musí být ohlášeny[32].

Zatímco způsob a struktura dokumentování případu porušení je na správci, ve věci obsahu jsou tu důležité prvky informací, které by měly být zaznamenány ve všech případech. Jak vyžaduje článek 33, odst. 5, správce musí uvést skutečnosti týkající se daného porušení jako příčiny, popis, co se stalo a jaké osobní údaje byly dotčeny. Také by měly být popsány účinky a důsledky porušení, jakož i správcem přijatá nápravná opatření.

WP29 doporučuje správcům, aby kromě těchto informací také dokumentovali odůvodnění svých rozhodnutí přijatých v reakci na porušení. Především, nebyl-li případ ohlášen, mělo by být dokladováno zdůvodnění. To by mělo uvádět důvody, proč je správce přesvědčen o tom, že je nepravděpodobné, že porušení bude mít za následek riziko pro práva a svobody jednotlivců[33]. Popřípadě, pokud se správce domnívá, že splnil veškeré podmínky článku 34, odst. 3, měl by být schopen to náležitě doložit.

Pokud správce ohlašuje porušení dozorovému úřadu opožděně, musí být schopen podat důvody odkladu; příslušná dokumentace může napomoci doložit, že toto zpoždění je oprávněné a není nadměrné.

Pokud správce oznamuje porušení dotčeným jednotlivcům, mělo by oznámení být věcně transparentní a sděleno účinným způsobem a včas. Uchování dokladu o oznámení pomůže správci předvést odpovědnost a doložit soulad.

Pro dosažení souladu s články 33 a 34 může být pro správce i zpracovatele výhodné mít dokumentovaný ohlašovací postup stanovující proces, podle kterého bude postupovat po odhalení případu porušení, včetně způsobu zvládnutí, vyřízení a nápravy incidentu, a také posouzení rizika a ohlášení případu. K předvedení souladu s Obecným nařízením může v tomto ohledu být užitečné doložit, že zaměstnanci byli informováni o existenci takových postupů a mechanismů a vědí, jak na případy porušení reagovat.

Je třeba poznamenat, že nesplnění povinnosti řádně porušení dokumentovat, může přivést dozorový úřad k uplatnění svých pravomocí podle článku 58 anebo uložit správní pokutu v souladu s článkem 83.

B. Role pověřence pro ochranu osobních údajů

Správce nebo zpracovatel budou mít pověřence pro ochranu osobních údajů (dále jen „pověřenec")[34], buď podle požadavku článku 37, nebo dobrovolně jako prvek osvědčené praxe. Článek 39 Obecného nařízení stanovuje pověřenci řadu povinných úkolů, nebrání však správci, aby případně uložil úkoly další.

V souvislosti s ohlašováním případů porušení je zvláště důležitý úkol spolupracovat s dozorovými úřady a působení jako kontaktní místo pro dozorový úřad a subjekty údajů. Dále je třeba poznamenat, že při ohlašování případu porušení zabezpečení dozorovému úřadu musí správce, podle článku 33, odst. 3, písm. b) uvést jméno a kontaktní údaje svého pověřence nebo jiného kontaktního místa. Tyto skutečnosti znamenají, že pověřenec by měl hrát důležitou roli při ohlašování události i během následného šetření dozorovým úřadem.

VI. Ohlašovací povinnosti podle jiných právních nástrojů

Vedle povinnosti ohlašovat a oznamovat případy porušení podle Obecného nařízení by správci měli mít povědomí o všech dalších požadavcích oznamovat porušení zabezpečení osobních údajů podle jiné související legislativy, která se na ně může vztahovat, což se může lišit v tom kterém členském státu. Patří sem následující právní akty:

---

[32] Správce si může vybrat, zda bude případy dokumentovat jako součást záznamů o činnostech zpracování vyžadovaných článkem 30. Oddělený registr není požadován za podmínky, že informace ohledně porušení je jako taková jasně identifikovatelná a lze ji na požádání vytáhnout.

[33] Viz recitál 85

[34] Viz Pokyny WP29 o pověřencích: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Nařízení (EU) 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Nařízení eIDAS)[35].

Tento materiál vyžaduje od poskytovatelů důvěryhodných služeb, aby svému dozorovému úřadu ohlašovali porušení.

- Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)[36].

Provozovatelé základních služeb i poskytovatelé digitálních služeb musí hlásit bezpečnostní incidenty, které se mohou týkat osobních údajů, příslušnému orgánu.

Příklad

Poskytovatel cloudové služby ohlašující incident podle směrnice NIS bude možná muset informovat i správce, je-li porušením zabezpečení osobních údajů dotčen. Podobně poskytovatel důvěryhodné služby ohlašující podle eIDAS může být také povinen ohlásit případ příslušnému dozorovému úřadu pro ochranu dat.

- Směrnice 2009/136/ES (Směrnice o právech občanů) a Nařízení 611/2013 (Nařízení o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů).

Poskytovatelé veřejně dostupných služeb elektronických komunikací v kontextu Směrnice 2002/58/ES[37] musí hlásit případy porušení příslušným národním orgánům.

Správci by dále měli znát všechny další právní, zdravotnické nebo profesní povinnosti ohlašování podle jiných platných režimů.

[35] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=CS

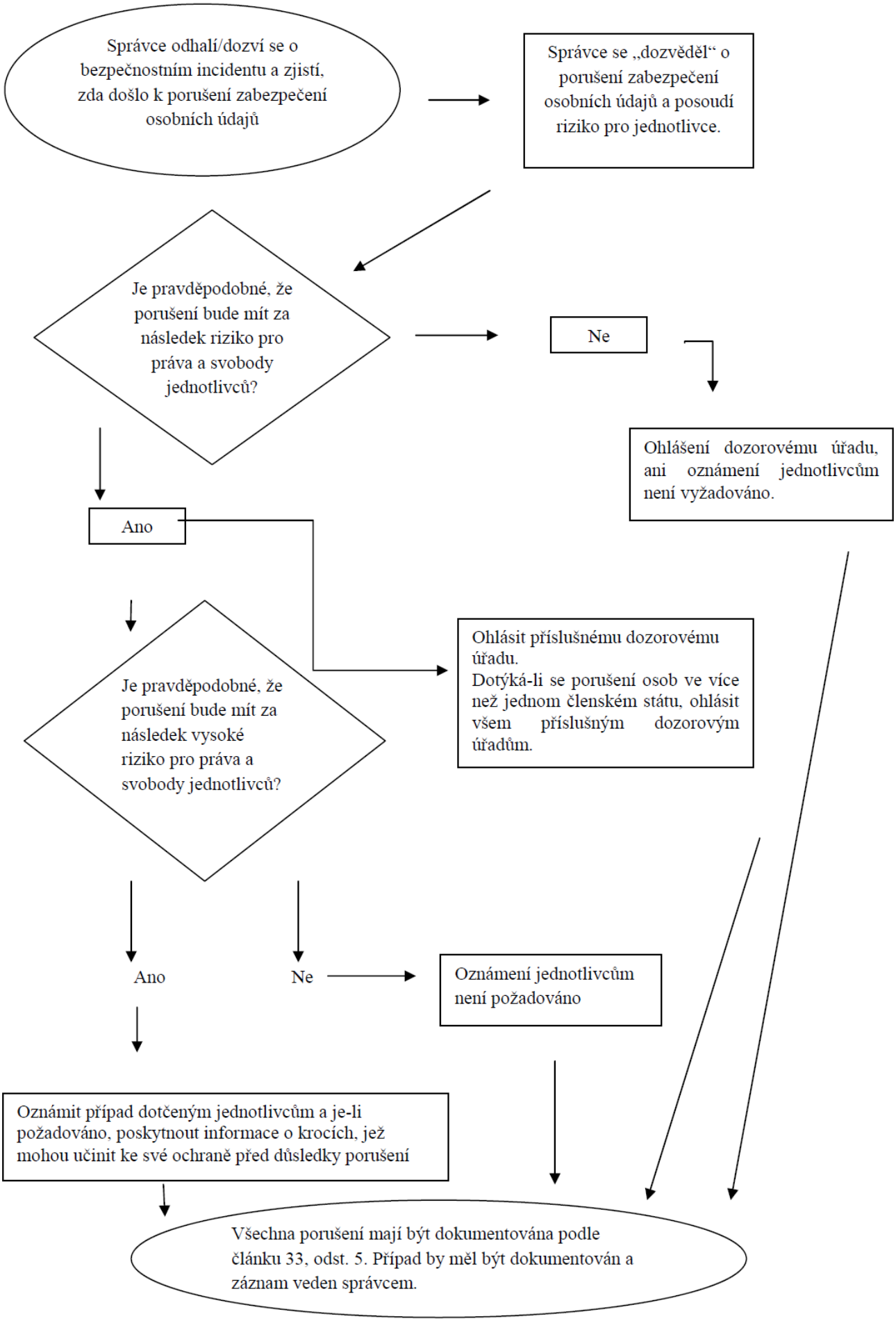
[36] Viz http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016L1148

[37] 10. ledna 2017 předložila Evropská Komise návrh Nařízení o soukromí a elektronických komunikacích, které nahradí Směrnici 2009/136/ES a zruší požadavky na ohlašování. Dokud však Evropský parlament tento návrh neschválí, zůstává nynější ohlašovací povinnost v platnosti, viz: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Neoficiální překlad

VII. **Příloha**

A. Diagram znázorňující požadavky na ohlášení



B. Příklady porušení zabezpečení a komu oznamovat

Následující příklady, byť se nejedná o vyčerpávající přehled scénářů, mají správcům pomoci při určování, zda musí za daných okolností případ porušení ohlašovat. Tyto příklady mohou také pomoci rozlišovat mezi rizikem a vysokým rizikem pro práva a svobody jednotlivců.

Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
I. Správce uložil záložní kopii archivu osobních údajů v zašifrované podobě na CD. Toto CD bylo odcizeno během vloupání.	Ne.	Ne.	Pokud jsou data zašifrovaná pomocí algoritmu na úrovni doby, data jsou zálohovaná a jedinečný klíč nebyl prozrazen, pak nemusí jít o hlásitelný případ. Je-li však později prolomen, ohlášení je nutné.
II. Osobní údaje jednotlivců jsou vyfiltrovány z bezpečné webové stránky provozované správcem během kybernetického útoku. Správce má zákazníky jen v jednom členském státě.	Ano, ohlásit případ příslušnému dozorovému úřadu je třeba, pokud hrozí možné důsledky pro jednotlivce.	Ano, oznámení jednotlivcům je nutné v závislosti na povaze dotčených osobních údajů a v případě vysoké závažnosti případných dopadů na jednotlivce.	Není-li riziko vysoké, doporučujeme, aby správce informoval subjekt údajů podle okolností případu. Oznámení například nemusí být vyžadováno, pokud jde o porušení důvěrnosti při zasílání novinek týkajících se televizní estrády, avšak může být nutné, pokud newsletter (zpravodaj) může vést k rozpoznání politických názorů subjektu údajů.
III. Krátký, jen několikaminutový výpadek proudu ve správcově call centru způsobí, že se s ním zákazníci nemohou spojit a získat přístup ke svým záznamům.	Ne.	Ne.	Nejedná se o porušení zabezpečení osobních údajů, které by bylo nutno ohlašovat, ale pořád je to incident, který je potřeba dokumentovat podle článku 33, odst. 5. Správce by měl vést náležité záznamy.
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
IV. Správce utrpí útok ransomwarem (vyděračským softwarem), čímž dojde k zašifrování všech jeho dat. K dispozici nejsou žádné zálohy a data nelze obnovit. Během šetření se přijde na to, že jedinou schopností ransomwaru bylo zašifrování údajů, a že systém neobsahoval žádný	Ano, ohlásit případ příslušnému dozorovému úřadu je nutné, pokud hrozí možné důsledky pro jednotlivce, neboť se jedná o ztrátu dostupnosti.	Ano, nutnost oznámit případ jednotlivcům bude záviset na povaze dotčených osobních údajů a na možných dopadech ztráty dostupnosti, jakož i na dalších pravděpodobných důsledcích.	Pokud by existovala záložní kopie a data by bylo možno v přijatelném čase obnovit, pak nebude třeba ohlašovat dozorovému úřadu ani oznamovat jednotlivci, protože by se nejednalo o trvalou ztrátu dostupnosti nebo důvěrnosti. Dozorový úřad však může zvážit provedení šetření k posouzení souladu s obecnějšími

jiný škodlivý software (malware).			požadavky stanovenými v článku 32.
V. Jednotlivec zavolá call centrum banky, aby ohlásil případ porušení zabezpečení. Volající totiž obdržel měsíční výpis z účtu někoho jiného. Správce zahájí krátké šetření (tj. ukončené např. během 24 hodin) a s dostatečnou jistotou zjistí, že došlo k porušení zabezpečení osobních údajů a zda se jedná o systémovou chybu, takže i další jednotlivci byli nebo by mohli být postiženi.	Ano.	Potřeba je oznámit to pouze dotčeným jednotlivcům za předpokladu, že existuje vysoké riziko a je jasné, že nikdo další nebyl zasažen.	Pokud bude dalším šetřením zjištěno, že bylo postiženo více osob, ohlášení dozorovému úřadu musí být učiněno a správce také musí záležitost dodatečně oznámit příslušným dalším jednotlivcům, existuje-li vysoké riziko.
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
VI. Nadnárodní online tržiště se stane obětí kybernetického útoku, přičemž útočník na internetu zveřejnění uživatelská jména, hesla a nákupní historii.	Ano, ohlášení dozorovému úřadu je nutné, týká-li se případ přeshraničního zpracování.	Ano, protože by mohlo mít za následek vysoké riziko.	Správce by měl podniknout kroky, např. vynutit resetování hesel u dotčených účtů a učinit i další kroky ke snížení rizika.
VII. Webhostingová firma (zpracovatel) zjistí chybu v kódu, který sleduje uživatelská oprávnění. Následkem této chyby může jakýkoliv uživatel vstoupit do účtu kteréhokoliv jiného uživatele.	Webhostingová firma, jsouce v postavení zpracovatele, musí věc bezodkladně ohlásit dotčeným klientům (správcům). Za předpokladu, že webhostingová firma provedla vlastní šetření, měli by mít dotčení správci důvodnou jistotu, zda každý z nich byl zasažen porušením a tedy se o případu „dozvěděl“ ve chvíli, kdy byl informován webhostingovou firmou (zpracovatelem). Správce pak musí případ ohlásit dozorovému úřadu.	Pokud není pravděpodobné, že by se mohlo objevit vysoké riziko pro jednotlivce, není potřeba jim případ oznámit.	Webhostingová firma (zpracovatel) musí vzít v úvahu veškeré další oznamovací povinnosti (např. podle Směrnice NIS). Neexistuje-li důkaz, že u konkrétního správce nebylo daného zranitelného místa zneužito, pak nemuselo dojít k porušení, které by bylo třeba ohlásit, ale mělo by být dokumentováno nebo být bráno jako záležitost, která je v nesouladu s článkem 32.
VIII. Zdravotní záznamy v nemocnici nejsou dostupné po dobu 30 hodin v důsledku kybernetického útoku.	Ano, nemocnice je povinna to ohlásit, vzhledem k vysokému riziku pro pacientovo zdraví a soukromí.	Ano, je třeba provést oznámení dotčeným jednotlivcům.	
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
IX. Osobní údaje 5000 studentů byly omylem	Ano, ohlásit případ dozorovému úřadu je	Ano, nutnost oznámení jednotlivcům bude záviset	

zaslány na nesprávný adresář čítající 1000 a více příjemců.	nutné.	na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	
X. E-mail v rámci přímého marketingu byl odeslán příjemcům v kolonce „komu“ nebo „kopie“, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.	Ano, ohlášení dozorovému úřadu může být povinné, jestliže byl postižen velký počet jednotlivců, došlo k odhalení citlivých údajů (např. adresář psychoterapeuta) nebo pokud existují jiné faktory představující vysoké riziko (např. zpráva obsahuje iniciační hesla).	Ano, nutnost oznámení jednotlivcům bude záviset na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	Ohlášení nemusí být nutné, pokud nedošlo k odhalení citlivých údajů a pokud došlo k odkrytí jen menšího počtu e-mailových adres.