NAŘÍZENÍ

NAŘÍZENÍ KOMISE (EU) č. 611/2013

ze dne 24. června 2013

o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) ([1]), a zejména na čl. 4 odst. 5 uvedené směrnice,

po konzultaci s Evropskou agenturou pro bezpečnost sítí a informací (ENISA),

po konzultaci s pracovní skupinou pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízenou článkem 29 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ([2]) (dále jen „pracovní skupina zřízená podle článku 29“),

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

(1) Směrnice 2002/58/ES harmonizuje předpisy členských států požadované pro zajištění rovnocenné úrovně ochrany základních práv a svobod, zejména práva na soukromí a zachování důvěrnosti informací, se zřetelem na zpracování osobních údajů v odvětví elektronických komunikací, a pro zajištění volného pohybu těchto údajů a elektronických komunikačních zařízení a služeb v Unii.

(2) Podle článku 4 směrnice 2002/58/ES jsou poskytovatelé veřejně dostupných služeb elektronických komunikací povinni oznámit narušení bezpečnosti osobních údajů příslušným vnitrostátním orgánům a v některých případech také dotčeným účastníkům a jednotlivcům. Narušení bezpečnosti osobních údajů je definováno v čl. 2 písm. i) směrnice 2002/58/ES jako narušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyzrazení nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti s poskytováním veřejně dostupné služby elektronických komunikací v Unii.

(3) Pro zajištění důsledného provádění opatření uvedených v čl. 4 odst. 2, 3 a 4 směrnice 2002/58/ES se v čl. 4 odst. 5 uvedeného nařízení Komise zmocňuje k přijetí technických prováděcích opatření týkajících se okolností, formátu a postupů, jež se vztahují na požadavky informování a oznamování podle uvedeného článku.

(4) Rozdílné požadavky členských států v tomto ohledu mohou vést k právní nejistotě, složitějším a zdlouhavějším postupům a značným administrativním nákladům poskytovatelů, kteří působí v přeshraničním styku. Komise proto zastává názor, že je nutné přijmout tato technická prováděcí opatření.

(5) Toto nařízení se omezuje na oznámení o narušení bezpečnosti osobních údajů, a proto nestanoví technická prováděcí opatření týkající se čl. 4 odst. 2 směrnice 2002/58/ES o informování účastníků v případě zvláštního rizika narušení bezpečnosti sítě.

(6) Z čl. 4 odst. 3 prvního pododstavce směrnice 2002/58/ES vyplývá, že poskytovatelé by měli oznámit příslušnému vnitrostátnímu orgánu všechny případy narušení bezpečnosti osobních údajů. Rozhodnutí, zda je či není třeba oznámit narušení příslušnému vnitrostátnímu orgánu, by proto nemělo být ponecháno na vůli poskytovatele. To by však nemělo bránit příslušnému vnitrostátnímu orgánu, aby v souladu s platnými právními předpisy nepřistoupil k vyšetřování některých narušení přednostně podle jejich důležitosti a nepodnikl kroky nezbytné k tomu, aby se zabránilo přílišnému nebo nedostatečnému hlášení o narušení bezpečnosti osobních údajů.

(7) Je třeba stanovit systém pro oznamování narušení bezpečnosti osobních údajů příslušnému vnitrostátnímu orgánu, který by za splnění některých podmínek sestával z různých etap, pro něž by platily konkrétní lhůty. Systém by měl zajistit, aby příslušný vnitrostátní orgán byl informován co nejdříve a co nejúplněji, aniž by se tím neodůvodněně bránilo poskytovateli ve snaze narušení vyšetřit a přijmout nezbytná opatření k jeho omezení a nápravě důsledků.

([1]) Úř. věst. L 201, 31.7.2002, s. 37.
([2]) Úř. věst. L 281, 23.11.1995, s. 31.

(8) Pouhé podezření, že došlo k narušení bezpečnosti osobních údajů, ani pouhé zjištění události bez dostatečných informací, které se ani přes největší úsilí nepodařilo poskytovateli získat, nepostačuje pro účely tohoto nařízení k tomu, aby bylo možné konstatovat, že došlo k odhalení narušení bezpečnosti osobních údajů. Zvláštní ohled je v této souvislosti třeba věnovat dostupnosti informací uvedených v příloze I.

(9) V souvislosti s uplatňováním tohoto nařízení by v případech narušení bezpečnosti osobních údajů s přeshraničním rozměrem měly příslušné vnitrostátní orgány mezi sebou spolupracovat.

(10) Toto nařízení nestanoví žádné upřesnění přehledu narušení bezpečnosti osobních údajů, které mají provozovatelé vést, protože v článku 4 směrnice 2002/58/ES je jeho obsah stanoven vyčerpávajícím způsobem. Poskytovatelé však při určování formátu přehledu mohou použít odkaz na toto nařízení.

(11) Všechny příslušné vnitrostátní orgány by měly poskytovatelům zpřístupnit bezpečné elektronické prostředky umožňující oznamovat narušení bezpečnosti osobních údajů ve společném formátu, a to na základě normy, jako je např. XML, který bude obsahovat údaje stanovené v příloze I v příslušných jazycích tak, aby všichni poskytovatelé v rámci Unie mohli používat obdobný postup oznamování bez ohledu na to, kde se nacházejí nebo kde došlo k narušení bezpečnosti osobních údajů. V této souvislosti by Komise podle potřeby měla usnadnit zavádění bezpečných elektronických prostředků pořádáním setkání s příslušnými vnitrostátními orgány.

(12) Při posuzování, zda by narušení bezpečnosti osobních údajů mohlo nepříznivě ovlivnit osobní údaje nebo soukromí účastníka nebo jednotlivce, je nutno vzít v úvahu zejména povahu a obsah dotyčných osobních údajů, zejména pokud jde o finanční informace, jako jsou např. údaje o kreditní kartě nebo bankovním účtu, zvláštní kategorie údajů podle čl. 8 odst. 1 směrnice 95/46/ES a některé údaje, které se konkrétně týkají poskytování telefonních a internetových služeb, tj. údaje o elektronické poště, lokalizační údaje, internetové soubory protokolů, historie navštívených webových stránek a podrobné rozpisy uskutečněných volání.

(13) Za výjimečných okolností, jestliže by oznámení účastníkovi nebo jednotlivci mohlo ohrozit řádné vyšetření narušení bezpečnosti osobních údajů, by poskytovatel měl mít možnost oznámení účastníkovi nebo jednotlivci pozdržet. V tomto ohledu mohou výjimečné okolnosti zahrnovat trestní vyšetřování, jakož i další narušení bezpečnosti osobních údajů, která nelze považovat za závažnou trestnou činnost, kvůli nimž však může být vhodné oznámení odložit. Příslušný vnitrostátní orgán by za všech okolností měl v každém jednotlivém případě a s ohledem na okolnosti posoudit, zda se oznámení odloží, nebo zda bude vyžadováno.

(14) Zatímco poskytovatelé by díky přímému smluvnímu vztahu měli mít kontaktní údaje svých účastníků, o ostatních jednotlivcích nepříznivě ovlivněných narušením bezpečnosti osobních údajů tyto informace mít nemusí. V takovém případě by poskytovatel měl mít možnost nejprve tyto jednotlivce informovat prostřednictvím oznámení zveřejněného v hlavních celostátních nebo regionálních médiích, např. v novinách, a následně jim tuto skutečnost co nejdříve oznámit jednotlivě, jak je stanoveno v tomto nařízení. Poskytovatel jako takový tedy není povinen zveřejnit informace v médiích, ale je oprávněn postupovat případně tímto způsobem, pokud stále ještě probíhá zjišťování totožnosti ovlivněných jednotlivců.

(15) Informace o narušení by se měla týkat pouze narušení a neměla by být spojena s jinými informacemi. Za přiměřený prostředek oznámení o narušení bezpečnosti osobních údajů by například nemělo být považováno uvedení informace o narušení bezpečnosti osobních údajů v běžné faktuře.

(16) Toto nařízení nestanoví žádná zvláštní technická ochranná opatření, která odůvodňují odchylku od povinnosti oznamovat narušení bezpečnosti osobních údajů účastníkům nebo jednotlivcům, neboť ta se mohou v důsledku technologického pokroku v průběhu času měnit. Komise by však měla mít možnost zveřejnit orientační seznam těchto zvláštních technických ochranných opatření v souladu s platnými postupy.

(17) Kódování nebo hašování nelze samo o sobě považovat za dostatečný způsob ochrany, který by poskytovatelům obecně umožňoval tvrdit, že splnili všechny všeobecné bezpečnostní povinnosti stanovené v článku 17 směrnice 95/46/ES. V tomto ohledu by poskytovatelé měli také provádět vhodná organizační a technická opatření na prevenci, odhalování a zamezení narušení bezpečnosti osobních údajů. Poskytovatelé by měli zvážit veškerá rizika, která mohou přetrvávat po provedení kontrol, aby bylo možné rozpoznat, kde může dojít k narušení bezpečnosti osobních údajů.

(18) Pokud provozovatel k poskytování služeb částečně používá jiného poskytovatele, např. pro účely účtování nebo řízení, tento jiný poskytovatel, který není v přímém smluvním vztahu s koncovým uživatelem, by neměl mít povinnost v případě narušení bezpečnosti osobních údajů podávat oznámení. Místo toho by měl uvědomit a informovat poskytovatele, s nímž má přímý smluvní vztah. To by mělo platit i v souvislosti s velkoobchodním

poskytováním služeb elektronických komunikací, kde obvykle velkoobchodní poskytovatel není v přímém smluvním vztahu s koncovým uživatelem.

(19) Směrnice 95/46/ES vymezuje obecný rámec pro ochranu osobních údajů v Evropské unii. Komise předložila návrh nařízení Evropského parlamentu a Rady (dále jako „nařízení o ochraně údajů"), které by mělo směrnici 95/46/ES nahradit. Navrhované nařízení o ochraně údajů by na základě čl. 4 odst. 3 směrnice 2002/58/ES zavedlo pro všechny správce povinnost oznamovat narušení bezpečnosti osobních údajů. Toto nařízení Komise je s tímto opatřením plně v souladu.

(20) Navrhované nařízení o ochraně údajů v omezeném rozsahu rovněž provádí technické úpravy ve směrnici 2002/58/ES s ohledem na změnu směrnice 95/46/ES na nařízení. Podstatné právní důsledky nového nařízení pro směrnici 2002/58/ES budou předmětem přezkumu, který provede Komise.

(21) Uplatňování tohoto nařízení by mělo být přezkoumáno tři roky po jeho vstupu v platnost a jeho obsah by měl být přezkoumán s ohledem na právní rámec, který bude v platnosti v uvedené době, včetně navrhovaného nařízení o ochraně údajů. Přezkum tohoto nařízení by měl v budoucnosti být, bude-li to možné, spojen s každým přezkumem směrnice 2002/58/ES.

(22) Uplatňování tohoto nařízení může být posuzováno mimo jiné na základě statistických údajů, které příslušné vnitrostátní orgány vedou o narušeních bezpečnosti osobních údajů, o nichž byly informovány. Tyto statistiky mohou zahrnovat např. informace o počtu narušení bezpečnosti osobních údajů oznámených příslušnému vnitrostátnímu orgánu, počtu případů narušení bezpečnosti osobních údajů oznámených účastníkovi nebo jednotlivci, době potřebné na vyřešení narušení bezpečnosti osobních údajů, a informace o tom, zda byla přijata technická ochranná opatření. Tyto statistiky by měly poskytovat Komisi a členským státům konzistentní a srovnatelné statistické údaje a neměly by odhalovat totožnost oznamujícího poskytovatele ani dotčených účastníků nebo jednotlivců. Komise může za tímto účelem rovněž pořádat pravidelná setkání s příslušnými vnitrostátními orgány a jinými zúčastněnými stranami.

(23) Opatření tohoto nařízení jsou v souladu se stanoviskem Komunikačního výboru,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Oblast působnosti

Toto nařízení se vztahuje na oznámení poskytovatelů veřejně dostupných služeb elektronických komunikací (dále jen „poskytovatel") o narušení bezpečnosti osobních údajů.

Článek 2

Oznámení příslušnému vnitrostátnímu orgánu

1. Poskytovatel oznámí všechna narušení bezpečnosti osobních údajů příslušnému vnitrostátnímu orgánu.

2. Poskytovatel oznámí narušení bezpečnosti osobních údajů příslušnému vnitrostátnímu orgánu nejpozději 24 hodin po zjištění narušení bezpečnosti osobních údajů, pokud je to proveditelné.

Poskytovatel ve svém oznámení příslušnému vnitrostátnímu orgánu uvede informace stanovené v příloze I.

Za zjištění narušení bezpečnosti osobních údajů se považuje situace, kdy poskytovatel získal dostatečné informace o tom, že došlo k bezpečnostní události, která měla za následek narušení osobních údajů, aby podal opodstatněné oznámení podle tohoto nařízení.

3. Jestliže nejsou k dispozici všechny informace stanovené v příloze I a je nutné další vyšetřování narušení bezpečnosti osobních údajů, může poskytovatel podat první oznámení příslušnému vnitrostátnímu orgánu nejpozději do 24 hodin po zjištění narušení bezpečnosti osobních údajů. Toto první oznámení příslušnému vnitrostátnímu orgánu musí obsahovat informace stanovené v příloze I oddíle 1. Poskytovatel je povinen podat příslušnému vnitrostátnímu orgánu co nejdříve, nejpozději do tří dnů po prvním oznámení, druhé oznámení. Toto druhé oznámení obsahuje informace stanovené v příloze I oddíle 2 a v případě potřeby aktualizuje již poskytnuté údaje.

Jestliže poskytovatel ani po vyšetřování nemůže ve lhůtě tří dnů od prvního oznámení poskytnout všechny informace, oznámí všechny informace, které má v této lhůtě k dispozici a předloží příslušnému vnitrostátnímu orgánu odůvodnění, proč musí být zbývající informace oznámeny později. Poskytovatel co možná nejdříve oznámí zbývající informace příslušnému vnitrostátnímu orgánu a v případě potřeby aktualizuje již poskytnuté údaje.

4. Příslušný vnitrostátní orgán poskytne všem poskytovatelům usazeným v dotčeném členském státě bezpečný elektronický prostředek pro oznamování narušení bezpečnosti osobních údajů a informace o postupech přístupu k němu a jeho používání. V zájmu snazšího uplatňování tohoto ustanovení Komise podle potřeby pořádá pravidelná setkání s příslušnými vnitrostátními orgány.

5. V případě, že se narušení bezpečnosti osobních údajů týká účastníků nebo jednotlivců z jiných členských států, než je členský stát příslušného vnitrostátního orgánu, jemuž bylo narušení bezpečnosti osobních údajů oznámeno, příslušný vnitrostátní orgán informuje orgány ostatních dotčených členských států.

Pro usnadnění uplatňování tohoto ustanovení Komise vytvoří a povede seznam příslušných vnitrostátních orgánů a příslušných kontaktních míst.

Článek 3

Oznámení účastníkovi nebo jednotlivci

1. Pokud by narušení bezpečnosti osobních údajů mohlo nepříznivě ovlivnit osobní údaje nebo soukromí účastníka nebo jednotlivce, musí poskytovatel kromě oznámení uvedeného v článku 2 toto porušení oznámit rovněž účastníkovi nebo jednotlivci.

2. Při posuzování, zda narušení bezpečnosti osobních údajů může mít nepříznivý vliv na osobní údaje nebo soukromí účastníka nebo jednotlivce, je nutno brát ohled zejména na tyto okolnosti:

a) povahu a obsah dotyčných osobních údajů, zejména pokud jde o finanční informace, zvláštní kategorie údajů podle čl. 8 odst. 1 směrnice 95/46/ES, jakož i lokalizační údaje, internetové soubory protokolů, historie navštívených webových stránek, údaje týkající se elektronické pošty a podrobné údaje o uskutečněných voláních;

b) pravděpodobné důsledky narušení bezpečnosti osobních údajů pro dotčeného účastníka nebo jednotlivce, zejména tehdy, kdy by porušení mohlo vést ke krádeži nebo zneužití, fyzické újmě, psychickému strádání, ponížení nebo poškození pověsti a

c) okolnosti narušení bezpečnosti osobních údajů, zejména pokud byly údaje odcizeny nebo pokud je poskytovateli známo, že údaje jsou v držení neoprávněné třetí strany.

3. Oznámení účastníkovi nebo jednotlivci musí být učiněno bez zbytečného odkladu po zjištění narušení bezpečnosti osobních údajů v souladu s čl. 2 odst. 2 třetím pododstavcem. Nesmí záviset na oznámení o narušení bezpečnosti osobních údajů příslušným vnitrostátním orgánům podle článku 2.

4. Poskytovatel ve svém oznámení účastníkovi nebo jednotlivci uvede informace stanovené v příloze II. Oznámení účastníkovi nebo jednotlivci musí být jasné a srozumitelné. Poskytovatel nesmí využít oznámení jako příležitost k propagaci nebo nabídce nových či doplňkových služeb.

5. Ve výjimečných případech, kdy oznámení účastníkovi nebo jednotlivci může ohrozit řádné vyšetření narušení bezpečnosti osobních údajů, má poskytovatel možnost po získání souhlasu příslušného vnitrostátního orgánu oznámení účastníkovi nebo jednotlivci pozdržet, dokud příslušný vnitrostátní orgán neusoudí, že je možné oznámit narušení bezpečnosti osobních údajů podle tohoto článku.

6. Poskytovatel oznámí účastníkovi nebo jednotlivci narušení bezpečnosti osobních údajů takovým způsobem, který umožňuje rychlé předání informací a který je podle nejnovějších poznatků náležitě zabezpečen. Informace o narušení by se měla týkat pouze narušení a neměla by být spojena s jinými informacemi.

7. Pokud poskytovatel, který je v přímém smluvním vztahu s koncovým uživatelem, ani přes vynaložené úsilí není schopen ve lhůtě uvedené v odstavci 3 určit všechny jednotlivce, kteří by narušením bezpečnosti osobních údajů mohli být nepříznivě ovlivněni, může v uvedené lhůtě tyto jednotlivce informovat prostřednictvím oznámení zveřejněného v hlavních celostátních nebo regionálních médiích v příslušných členských státech. Uvedená oznámení musí obsahovat informace stanovené v příloze II, v případě potřeby ve stručné formě. V takovém případě poskytovatel pokračuje v úsilí vedoucím k identifikaci těchto jednotlivců a co nejdříve jim oznámí informace uvedené v příloze II.

Článek 4

Technická ochranná opatření

1. Odchylně od čl. 3 odst. 1 se oznámení o narušení bezpečnosti osobních údajů dotčenému účastníkovi nebo jednotlivci nevyžaduje, pokud poskytovatel ke spokojenosti příslušného vnitrostátního orgánu prokázal, že zavedl náležitá technická ochranná opatření a že tato opatření byla na údaje, jichž se narušení bezpečnosti týká, použita. Tato technická ochranná opatření zajistí, aby údaje nebyly srozumitelné pro nikoho, kdo není k přístupu k nim oprávněn.

2. Údaje se považují za nesrozumitelné, jestliže:

a) byly bezpečně zašifrovány normalizovaným algoritmem, klíč použitý k dešifrování údajů nebyl žádným narušením bezpečnosti ohrožen a byl vytvořen tak, aby nemohl být dostupnými technickými prostředky odhalen nikým, kdo k němu nemá právo přístupu, nebo

b) byly nahrazeny svou zahašovanou hodnotou vypočítanou pomocí normalizované kryptografické hašovací funkce s klíčem, klíč použitý k hašování údajů nebyl ohrožen žádným narušením bezpečnosti a byl vytvořen tak, aby nemohl být dostupnými technickými prostředky odhalen nikým, kdo k němu nemá právo přístupu.

3. Komise může po konzultaci s příslušnými vnitrostátními orgány prostřednictvím pracovní skupiny zřízené podle článku 29, Evropskou agenturou pro bezpečnost sítí a informací a evropským inspektorem ochrany údajů zveřejnit orientační seznam vhodných technických ochranných opatření uvedených v odstavci 1 v souladu s platnými postupy.

Článek 5

Použití jiného poskytovatele

Jestliže je jiný poskytovatel smluvně zavázán, aby poskytl část služeb elektronických komunikací, aniž by byl v přímém smluvním vztahu s účastníky, tento další poskytovatel v případě, že došlo k narušení bezpečnosti osobních údajů, okamžitě informuje smluvního poskytovatele.

Článek 6

Podávání zpráv a přezkum

Do tří let od vstupu tohoto nařízení v platnost Komise předloží zprávu o uplatňování tohoto nařízení, jeho účinnosti a dopadu na poskytovatele, účastníky a jednotlivce. Na základě uvedené zprávy Komise toto nařízení přezkoumá.

Článek 7

Vstup v platnost

Toto nařízení vstupuje v platnost dne 25. srpna 2013.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 24. června 2013.

Za Komisi

José Manuel BARROSO

předseda

PŘÍLOHA I

Obsah oznámení příslušnému vnitrostátnímu orgánu

Oddíl 1

Údaje o totožnosti poskytovatele

1. Jméno poskytovatele

2. Označení a kontaktní údaje inspektora ochrany údajů nebo jiného kontaktního místa, kde lze získat bližší informace

3. Zda se jedná o první nebo druhé oznámení

Prvotní informace o narušení bezpečnosti osobních údajů (doplněné případně v pozdějším oznámení)

4. Datum a čas vzniku události (pokud jsou známy: případně lze uvést odhad) a zjištění události

5. Okolnosti narušení bezpečnosti osobních údajů (např. ztráta, krádež, kopírování)

6. Povaha a obsah dotčených osobních údajů

7. Technická a organizační opatření, která byla (nebo mají být) použita poskytovatelem na dotčené osobních údaje

8. Příslušné použití jiných poskytovatelů (v náležitých případech)

Oddíl 2

Další informace o narušení bezpečnosti osobních údajů

9. Souhrnná zpráva o události, která způsobila narušení bezpečnosti osobních údajů (včetně místa, v němž k narušení došlo, a dotčeného nosiče dat)

10. Počet dotčených účastníků nebo jednotlivců

11. Možné důsledky a možné nepříznivé účinky na účastníky nebo jednotlivce

12. Technická a organizační opatření, jež poskytovatel přijal ke zmírnění možných nepříznivých účinků

Případné další oznámení účastníkům nebo jednotlivcům

13. Obsah oznámení

14. Použité sdělovací prostředky

15. Počet účastníků nebo jednotlivců, jimž bylo sděleno oznámení

Možné přeshraniční aspekty

16. Narušení bezpečnosti osobních údajů týkající se účastníků nebo jednotlivců v jiných členských státech

17. Oznámení sdělené příslušným orgánům v jiných státech

PŘÍLOHA II

Obsah oznámení účastníkovi nebo jednotlivci

1. Jméno poskytovatele

2. Označení a kontaktní údaje inspektora ochrany údajů nebo jiného kontaktního místa, kde lze získat bližší informace

3. Souhrnná zpráva o události, která způsobila narušení bezpečnosti osobních údajů

4. Odhadované datum události

5. Povaha a obsah dotčených osobních údajů podle čl. 3 odst. 2

6. Pravděpodobné důsledky narušení bezpečnosti osobních údajů pro dotčeného účastníka nebo jednotlivce podle čl. 3 odst. 2

7. Okolnosti narušení bezpečnosti osobních údajů podle čl. 3 odst. 2

8. Opatření, jež poskytovatel v souvislosti s narušením bezpečnosti osobních údajů přijal

9. Opatření doporučená poskytovatelem ke zmírnění možných nepříznivých účinků