

NARIADENIA

NARIADENIE KOMISIE (EÚ) č. 611/2013

z 24. júna 2013

o opatreniach uplatniteľných na oznamovanie prípadov porušenia ochrany osobných údajov na základe smernice Európskeho parlamentu a Rady 2002/58/ES o súkromí a elektronických komunikáciách

EURÓPSKA KOMISIA,

alebo inak spracúvajú v súvislosti s poskytovaním verejne dostupnej elektronickej komunikačnej služby v Únii.

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcu sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách)⁽¹⁾, a najmä na jej článok 4 ods. 5,

(3) S cieľom zabezpečiť konzistentné vykonávanie opatrení uvedených v článku 4 ods. 2, 3 a 4 smernice 2002/58/ES sa článkom 4 ods. 5 danej smernice Komisia splnomocňuje na prijímanie technických vykonávacích opatrení týkajúcich sa okolností, formy a postupov, ktoré sa vzťahujú na požiadavky súvisiace s informáciami a oznámeniami podľa daného článku.

po porade s Európskou agentúrou pre bezpečnosť sietí a informácií (ENISA),

(4) Rozličné požiadavky jednotlivých členských štátov v danom ohľade môžu viesť k právnej neistote, zložitejším a zdĺhavejším postupom a značným administratívnym nákladom pre cezhranične pôsobiacich poskytovateľov. Komisia preto považuje za potrebné prijať uvedené technické vykonávacie opatrenia.

po porade s pracovnou skupinou pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov zriadenou podľa článku 29 smernice Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe takýchto údajov⁽²⁾ (článok 29 Pracovná skupina),

(5) Toto nariadenie sa obmedzuje na oznamovanie prípadov porušenia ochrany osobných údajov, preto sa ním nestanovujú technické vykonávacie opatrenia týkajúce sa článku 4 ods. 2 smernice 2002/58/ES o informovaní príslušných účastníkov v prípade osobitného rizika narušenia bezpečnosti siete.

po porade s európskym dozorným úradníkom pre ochranu údajov (EDPS),

keďže:

(6) Z prvého pododseku odseku 3 článku 4 smernice 2002/58/ES vyplýva, že poskytovatelia by mali oznamovať príslušnému vnútroštátnemu orgánu všetky prípady porušenia ochrany osobných údajov. Poskytovateľ by preto nemal mať diskrečnú právomoc rozhodnúť, či príslušnému vnútroštátnemu orgánu porušenie oznámi alebo nie. Dotknutému príslušnému vnútroštátnemu orgánu by to však nemalo brániť prednostne vyšetrovať určité porušenia ochrany spôsobom, ktorý považuje za vhodný v súlade s uplatniteľnými právnymi predpismi, a prijímať opatrenia potrebné na predchádzanie nedostatočnému alebo nadmernému nahlasovaniu porušení ochrany osobných údajov.

(1) Smernicou 2002/58/ES sa ustanovuje harmonizácia vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernosc, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore a na zabezpečenie voľného pohybu takých údajov a elektronických komunikačných zariadení a služieb v Únii.

(2) Podľa článku 4 smernice 2002/58/ES poskytovateľ verejne dostupnej elektronickej komunikačnej služby musí porušenie ochrany osobných údajov oznámiť príslušným vnútroštátnym orgánom a v určitých prípadoch aj účastníkom a dotknutým jednotlivcom. Pojem porušenie osobných údajov je vymedzený v článku 2 písm. i) smernice 2002/58/ES ako porušenie bezpečnosti, ktoré má za následok náhodné alebo nezákonné zničenie, stratu, zmenu nedovolené zverejnenie alebo sprístupnenie osobných údajov, ktoré sa prenášajú, ukladajú

(7) Na oznamovanie porušení ochrany osobných údajov príslušnému vnútroštátnemu orgánu je vhodné stanoviť systém, ktorý v prípade splnenia určitých podmienok pozostáva z rôznych etáp, pričom na každú z nich sa vzťahujú určité lehoty. Cieľom systému je zabezpečiť, že príslušný vnútroštátny orgán dostane informácie čo možno najskôr a čo možno najúplnejšie, avšak bez toho, aby to poskytovateľovi nadmieru prekážalo v jeho úsilí o vyšetrenie daného porušenia a v prijatí potrebných opatrení na jeho obmedzenie a nápravu vzniknutých dôsledkov.

(1) Ú. v. ES L 201, 31.7.2002, s. 37.

(2) Ú. v. ES L 281, 23.11.1995, s. 31.

- (8) Ani samotné podozrenie, že došlo k porušeniu ochrany osobných údajov, ani samotné zistenie narušenia bezpečnosti bez dostatočných informácií, ktoré sa poskytovateľovi ani napriek najväčšej snahe vynaloženej v tomto smere nepodarilo získať, nepostačuje na účely tohto nariadenia na skonštatovanie, že sa zistilo porušenie ochrany osobných údajov. V tejto súvislosti by sa mal brať osobitný ohľad na dostupnosť informácií uvedených v prílohe I.
- (9) Pri uplatňovaní tohto nariadenia by príslušné vnútroštátne orgány mali spolupracovať v prípadoch, keď porušenia ochrany osobných údajov sú cezhraničnej povahy.
- (10) V tomto nariadení sa nestanovuje ďalšie bližšie určenie zoznamu prípadov porušení ochrany osobných údajov, ktorý majú poskytovatelia viesť, keďže v článku 4 smernice 2002/58/ES sa jeho obsah uvádza vyčerpávajúco. Poskytovatelia však môžu na určenie formátu uvedeného zoznamu použiť toto nariadenie.
- (11) Všetky príslušné vnútroštátne orgány by mali dať poskytovateľom k dispozícii bezpečné elektronické prostriedky na oznamovanie porušení ochrany osobných údajov v spoločnom formáte, založenom na norme ako napríklad XML, obsahujúcom informácie uvedené v prílohe I v príslušných jazykoch, aby všetci poskytovatelia v Únii mohli podávať oznámenia obdobným postupom bez ohľadu na to, kde sa nachádzajú alebo kde došlo k porušeniu ochrany osobných údajov. V tejto súvislosti by Komisia prípadne mala uľahčiť zavádzanie bezpečných elektronických prostriedkov prostredníctvom zvolávania zasadnutí s príslušnými vnútroštátnymi orgánmi.
- (12) Pri posudzovaní, či sa porušenie ochrany osobných údajov pravdepodobne nepriaznivo dotkne osobných údajov alebo súkromia účastníka alebo jednotlivca, by sa mala zohľadniť predovšetkým povaha a obsah dotknutých osobných údajov, predovšetkým ak ide o finančné informácie, akými sú údaje o kreditnej karte alebo údaje o bankovom účte; osobitné kategórie údajov uvedené v článku 8 ods. 1 smernice 95/46/ES; a určité údaje konkrétne súvisiace s poskytovaním telefónnych alebo internetových služieb, t. j. údaje o elektronickej pošte, lokalizačné dáta, internetové logovacie súbory, záznamy o prezeraných webových stránkach a zoznamy jednotlivých hovorov.
- (13) Za výnimočných okolností by sa poskytovateľovi malo povoliť odložiť oznámenie účastníkovi alebo jednotlivcovi, ak oznámenie účastníkovi alebo jednotlivcovi môže ohroziť riadne vyšetrenie daného porušenia ochrany osobných údajov. K výnimočným okolnostiam v tejto súvislosti môžu patriť trestnoprávne vyšetrenia, ako aj iné porušenia ochrany osobných údajov, ktoré nezodpovedajú závažnej trestnej činnosti, ale pri ktorých môže byť vhodné oznámenie odložiť. Posúdenie v každom jednotlivom prípade a so zreteľom na okolnosti, či pristúpiť na odloženie oznámenia, alebo ho vyžadovať, by každopádne malo byť na príslušnom vnútroštátnom orgáne.
- (14) Poskytovatelia by síce vzhľadom na ich priamy zmluvný vzťah mali mať kontaktné údaje svojich účastníkov, no takéto informácie nemusia existovať v prípade iných jednotlivcov nepriaznivo dotknutých daným porušením ochrany osobných údajov. V takom prípade by sa poskytovateľovi malo povoliť informovať týchto jednotlivcov najprv prostredníctvom inzercie v hlavných celoštátnych alebo regionálnych médiách, napríklad novinách, po ktorej bude čo najskôr nasledovať individuálne oznámenie podľa ustanovení v tomto nariadení. Poskytovateľ teda nie je povinný oznamovať prostredníctvom médií, ale ak si to želá, má skôr poverenie postupovať tak, kým ešte stále prebieha zisťovanie totožnosti všetkých dotknutých jednotlivcov.
- (15) Informácie o porušení ochrany by sa mali venovať porušeniu a nemali by sa spájať s informáciami na inú tému. Za adekvátny spôsob informovania o porušení ochrany osobných údajov by sa nemalo považovať napríklad začlenenie informácie o porušení ochrany osobných údajov do pravidelnej faktúry.
- (16) V tomto nariadení sa nestanovujú konkrétne technologické ochranné opatrenia, ktoré odôvodňujú odchýlku od povinnosti oznamovať účastníkom alebo jednotlivcom porušenia ochrany osobných údajov, keďže tieto opatrenia sa môžu časom meniť v dôsledku technologického pokroku. Komisia by však mala byť schopná uviesť orientačný zoznam takýchto konkrétnych technologických ochranných opatrení v súlade s platnými postupmi.
- (17) Implementácia kódovania ani hašovania by sa nemala sama o sebe považovať za dostatočnú na to, aby oprávňovala poskytovateľov na širšie tvrdenie, že spĺňajú všeobecné bezpečnostné povinnosti uvedené v článku 17 smernice 95/46/ES. V tomto ohľade by poskytovatelia mali takisto zaviesť primerané organizačné a technické opatrenia na zabránenie porušeniam ochrany osobných údajov a na ich zisťovanie a izolovanie. Poskytovatelia by mali zvážiť všetky riziká, ktoré by mohli pretrvávajúť po zavedení kontrol, aby porozumeli tomu, kde môže prípadne dôjsť k porušeniam ochrany osobných údajov.
- (18) Keď poskytovateľ využíva iného poskytovateľa na vykonanie časti služby, pokiaľ ide napríklad o účtovné alebo riadiace úlohy, tento iný poskytovateľ, ktorý nemá žiadny

priamy zmluvný vzťah s koncovým užívateľom, by nemal mať povinnosť podávať oznámenia v prípade, že dôjde k porušeniu ochrany osobných údajov. Namiesto toho by mal upozorniť a informovať poskytovateľa, s ktorým má priamy zmluvný vzťah. Malo by to platiť aj v rámci veľkoobchodného poskytovania elektronických komunikačných služieb, keď veľkoobchodný poskytovateľ v zásade nemá priamy zmluvný vzťah s koncovým užívateľom.

- (19) Smernicou 95/46/ES sa vymedzuje všeobecný rámec pre ochranu osobných údajov v Európskej únii. Komisia predložila návrh nariadenia Európskeho parlamentu a Rady s cieľom nahradiť smernicu 95/46/ES (ďalej len nariadenie o ochrane údajov). Navrhovaným nariadením o ochrane údajov by sa na základe článku 4 ods. 3 smernice 2002/58/ES zaviedla povinnosť pre všetkých prevádzkovateľov oznamovať porušenia ochrany osobných údajov. Toto nariadenie Komisie je plne v súlade s navrhovaným opatrením.
- (20) V navrhovanom nariadení o ochrane údajov sa zároveň vykonala obmedzená zmena technických úprav v smernici 2002/58/ES, aby sa zohľadnila zmena smernice 95/46/ES na nariadenie. Podstatné právne dôsledky nového nariadenia pre smernicu 2002/58/ES budú predmetom preskúmania Komisie.
- (21) Uplatňovanie tohto nariadenia by sa malo preskúmať po troch rokoch od nadobudnutia jeho účinnosti a jeho obsah by sa mal preskúmať z pohľadu právneho rámca platného v danom čase, vrátane navrhovaného nariadenia o ochrane údajov. Preskúmanie tohto nariadenia by malo byť podľa možnosti spojené s každým budúcim preskúmaním smernice 2002/58/ES.
- (22) Uplatňovanie tohto nariadenia sa môže posúdiť okrem iného na základe akýchkoľvek štatistických údajov, ktoré uchovávajú príslušné vnútroštátne orgány o porušení ochrany osobných údajov, ktoré im boli oznámené. Tieto štatistické údaje môžu zahŕňať napríklad informácie o počte porušení ochrany osobných údajov oznámených danému príslušnému vnútroštátnemu orgánu, počte porušení ochrany osobných údajov oznámených účastníkovi alebo jednotlivcovi, čase potrebnom na vyriešenie porušenia ochrany osobných údajov a o tom, či boli prijaté technické ochranné opatrenia. Uvedené štatistiky by mali Komisii a členským štátom poskytovať konzistentné a porovnateľné štatistické údaje a nemali by odhaľovať totožnosť oznamujúceho poskytovateľa ani dotknutých účastníkov či jednotlivcov. Komisia môže na tieto účely zároveň organizovať pravidelné stretnutia s príslušnými vnútroštátnymi orgánmi a inými zainteresovanými stranami.
- (23) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom komunikačného výboru,

PRIJALA TOTO NARIADENIE:

Článok 1

Rozsah pôsobnosti

Toto nariadenie sa uplatňuje na oznámenia poskytovateľov verejne dostupnej elektronickej komunikačnej služby (ďalej len „poskytovateľ“) o porušení ochrany osobných údajov.

Článok 2

Oznamovanie príslušnému vnútroštátnemu orgánu

1. Poskytovateľ oznámi každé porušenie ochrany osobných údajov príslušnému vnútroštátnemu orgánu.
2. Poskytovateľ oznámi porušenie ochrany osobných údajov príslušnému vnútroštátnemu orgánu najneskôr do 24 hodín po zistení porušenia ochrany osobných údajov, ak je to uskutočniteľné.

Do oznámenia určeného príslušnému vnútroštátnemu orgánu poskytovateľ zahrnie informácie stanovené v prílohe I.

Za zistenie porušenia ochrany osobných údajov sa pokladá situácia, keď poskytovateľ nadobudol vedomosť o tom, že došlo k narušeniu bezpečnosti, ktoré viedlo k zneužitiu osobných údajov, dostávajúcu na to, aby mohol podať zmysluplné oznámenie podľa požiadaviek v tomto nariadení.

3. Ak nie sú dostupné všetky informácie stanovené v prílohe 1 a je nevyhnutné ďalšie vyšetrovanie porušenia ochrany osobných údajov, poskytovateľovi sa povoľuje poskytnúť prvotné oznámenie príslušnému vnútroštátnemu orgánu najneskôr 24 hodín po zistení porušenia ochrany osobných údajov. Toto prvotné oznámenie príslušnému vnútroštátnemu orgánu obsahuje informácie stanovené v oddiele 1 prílohy I. Čo najskôr, najneskôr však do troch dní po prvotnom oznámení, podá poskytovateľ príslušnému vnútroštátnemu orgánu druhé oznámenie. Toto druhé oznámenie obsahuje informácie stanovené v oddiele 2 prílohy I a v prípade potreby sa v ňom aktualizujú predtým poskytnuté informácie.

Keď poskytovateľ ani napriek vyšetrovaniam nie je schopný poskytnúť v trojdňovej lehote od zaslania prvotného oznámenia všetky informácie, oznámi tie informácie, ktoré má v danej lehote k dispozícii, a predloží príslušnému vnútroštátnemu orgánu podložené odôvodnenie, prečo zvyšné informácie oznámi neskôr. Poskytovateľ čo najskôr oznámi zvyšné informácie príslušnému vnútroštátnemu orgánu a v prípade potreby aktualizuje predtým poskytnuté informácie.

4. Príslušný vnútroštátny orgán poskytne všetkým poskytovateľom usadeným v dotknutom členskom štáte bezpečný elektronický prostriedok na oznamovanie porušenia ochrany osobných údajov a informácie o postupoch prístupu k nemu a jeho používania. Komisia v prípade potreby zorganizuje stretnutia s príslušnými vnútroštátnymi orgánmi s cieľom uľahčiť uplatňovanie tohto ustanovenia.

5. Keď sa porušenie ochrany osobných údajov dotkne účastníkov alebo jednotlivcov z iných členských štátov než z členského štátu príslušného vnútroštátneho orgánu, ktorému sa porušenie ochrany osobných údajov oznámilo, daný príslušný vnútroštátny orgán informuje vnútroštátne orgány ostatných dotknutých členských štátov.

Na ľahšie uplatňovanie tohto ustanovenia Komisia vypracuje a udržiava zoznam príslušných vnútroštátnych orgánov a zodpovedajúcich kontaktných miest.

Článok 3

Oznámenie účastníkovi alebo jednotlivcovi

1. Ak je pravdepodobné, že porušenie ochrany osobných údajov nepriaznivo ovplyvní osobné údaje alebo súkromie účastníka alebo jednotlivca, poskytovateľ okrem oznámenia uvedeného v článku 2 oznámi takéto porušenie aj účastníkovi alebo jednotlivcovi.

2. To, či porušenie ochrany osobných údajov pravdepodobne nepriaznivo ovplyvní osobné údaje alebo súkromie účastníka alebo jednotlivca, sa posúdi so zohľadnením najmä týchto okolností:

1. povaha a obsah dotknutých osobných údajov, predovšetkým ak ide o finančné informácie, osobitné kategórie údajov uvedené v článku 8 ods. 1 smernice 95/46/ES, ako aj lokalizačné údaje, internetové logovacie súbory, záznamy o prezeraných webových stránkach, údaje o elektronickej pošte a zoznamy jednotlivých hovorov;
2. pravdepodobné dôsledky porušenia ochrany osobných údajov pre dotknutého účastníka alebo jednotlivca, najmä ak by porušenie mohlo viesť ku krádeži alebo zneužitiu identity, fyzickej ujme, psychickému utrpeniu, poníženiu alebo poškodeniu povesti, ako aj
3. okolnosti porušenia ochrany osobných údajov, najmä ak boli údaje odcudzené alebo ak poskytovateľ vie, že údaje má v držbe neoprávnená tretia strana.
3. Oznámenie účastníkovi alebo jednotlivcovi sa vykoná bez zbytočného odkladu po zistení porušenia ochrany osobných údajov, ako sa uvádza v článku 2 ods. 2 treťou pododseku. Nemalo by to závisieť od oznámenia porušenia ochrany osobných údajov príslušnému vnútroštátnemu orgánu uvedeného v článku 2.
4. Do oznámenia určeného účastníkovi alebo jednotlivcovi poskytovateľ zahrnie informácie stanovené v prílohe II. Jazyk oznámenia určeného účastníkovi alebo jednotlivcovi musí byť jasný a ľahko zrozumiteľný. Poskytovateľ nesmie využiť oznámenie ako príležitosť na propagáciu alebo reklamu nových ani doplnkových služieb.
5. Za výnimočných okolností, keď oznámenie účastníkovi alebo jednotlivcovi môže ohroziť riadne vyšetrovanie porušenia ochrany osobných údajov, poskytovateľovi sa po získaní súhlasu od príslušného vnútroštátneho orgánu povoľuje odložiť zaslanie oznámenia účastníkovi alebo jednotlivcovi dovtedy,

kým príslušný vnútroštátny orgán nepovažuje za možné oznámiť porušenie ochrany osobných údajov v súlade s týmto článkom.

6. Poskytovateľ oznámi účastníkovi alebo jednotlivcovi porušenie ochrany osobných údajov takými komunikačnými prostriedkami, ktorými sa zabezpečí rýchle doručenie informácií a ktoré sú podľa najnovších poznatkov v danej oblasti náležite zabezpečené. Informácie o porušení sú venované len danému porušeniu a nespájajú sa s informáciami na iné témy.

7. Keď poskytovateľ, ktorý má priamy zmluvný vzťah s koncovým užívateľom, ani napriek vynaloženému primeranému úsiliu nie je schopný v lehote uvedenej v odseku 3 identifikovať všetkých jednotlivcov, ktorých by sa pravdepodobne mohlo nepriaznivo dotknúť dané porušenie ochrany osobných údajov, môže v uvedenej lehote informovať týchto jednotlivcov prostredníctvom inzercie uverejnenej v hlavných celoštátnych alebo regionálnych médiách v príslušných členských štátoch. Takáto inzercia obsahuje informácie uvedené v prílohe II, v prípade potreby v stručnej forme. Poskytovateľ v takom prípade pokračuje v primeranom úsilí identifikovať daných jednotlivcov a oznámiť im informácie uvedené v prílohe II čo najskôr.

Článok 4

Technické ochranné opatrenia

1. Odchylné od článku 3 ods. 1 oznámenie o porušení ochrany osobných údajov dotknutému účastníkovi alebo jednotlivcovi sa nevyžaduje, ak poskytovateľ preukázal k spokojnosti príslušného vnútroštátneho orgánu, že vykonal primerané technologicke ochranné opatrenia a že tieto opatrenia sa uplatnili na údaje dotknuté porušením bezpečnosti. Takými opatreniami technologickej ochrany sa zabezpečí, aby sa údaje stali nečitateľné pre všetky osoby bez oprávneného prístupu k nim.
2. Údaje sa považujú za nečitateľné, ak:
 1. boli bezpečne zakódované normalizovaným algoritmom, kľúč používaný na odkódovanie údajov nebol poškodený žiadnym porušením bezpečnosti a tento kľúč bol vytvorený tak, aby ho nikto, kto k nemu nemá prístupové právo, nemohol dostupnými technickými prostriedkami zistiť, alebo
 2. boli nahradené ich hašovanou hodnotou vypočítanou pomocou normalizovanej kryptografickej hašovacej funkcie s kľúčom, pričom kľúč použitý na hašovanie údajov nebol poškodený žiadnym porušením bezpečnosti a tento kľúč bol vytvorený tak, aby ho nikto, kto k nemu nemá prístupové právo, nemohol dostupnými technickými prostriedkami zistiť.
3. Komisia môže po porade s príslušnými vnútroštátnymi orgánmi prostredníctvom pracovnej skupiny zriadenej článkom 29, Európskou agentúrou pre bezpečnosť sietí a informácií a európskym dozorným úradníkom pre ochranu údajov uverejniť orientačný zoznam primeraných technologickej ochranných opatrení uvedených v odseku 1 v súlade s platnými postupmi.

Článok 5**Využívanie iného poskytovateľa**

Ak sa časť elektronickej komunikačnej služby poskytuje na základe zmluvy s iným poskytovateľom, pričom tento nemá priamy zmluvný vzťah s účastníkmi, tento iný poskytovateľ bezodkladne informuje zadávajúceho poskytovateľa v prípade porušenia ochrany osobných údajov.

Článok 6**Podávanie správ a preskúmanie**

Do troch rokov od nadobudnutia účinnosti tohto nariadenia Komisia predloží správu o uplatňovaní tohto nariadenia, jeho účinnosti a vplyve na poskytovateľov, účastníkov a jednotlivcov. Komisia na základe uvedenej správy preskúma toto nariadenie.

Článok 7**Nadobudnutie účinnosti**

Toto nariadenie nadobúda účinnosť 25. augusta 2013.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 24. júna 2013

Za Komisiu
predseda
José Manuel BARROSO

PRÍLOHA I

Obsah oznámenia určeného príslušnému vnútroštátnemu orgánu**Oddiel 1***Identifikačné údaje poskytovateľa*

1. meno/názov poskytovateľa;
2. údaje o totožnosti a kontaktné údaje úradníka pre ochranu údajov alebo iné kontaktné miesto, kde možno získať viac informácií;
3. spresnenie, či ide o prvé alebo druhé oznámenie;

Prvotné informácie o porušení ochrany osobných údajov (na prípadné doplnenie v neskorších oznámeniach)

4. dátum a čas udalosti (ak sú známe, prípadne sa môžu odhadnúť) a dátum a čas zistenia udalosti;
5. okolnosti porušenia ochrany osobných údajov (napr. strata, krádež, kopírovanie);
6. povaha a obsah dotknutých osobných údajov;
7. technické a organizačné opatrenia, ktoré poskytovateľ uplatnil (alebo má uplatniť) na dotknuté osobné údaje;
8. (v prípade potreby) príslušné využívanie iných poskytovateľov;

Oddiel 2*Ďalšie informácie o porušení ochrany osobných údajov*

9. zhrnutie udalosti, ktorá spôsobila porušenie ochrany osobných údajov (vrátane fyzického miesta, kde došlo k porušeniu a dotknutého pamäťového média);
10. počet dotknutých účastníkov alebo jednotlivcov;
11. možné dôsledky a možné nepriaznivé účinky na účastníkov alebo jednotlivcov;
12. technické a organizačné opatrenia, ktoré poskytovateľ prijal na zmiernenie možných nepriaznivých účinkov;

Prípadné ďalšie oznámenie účastníkom alebo jednotlivcom

13. obsah oznámenia;
14. použité komunikačné prostriedky;
15. počet účastníkov alebo jednotlivcov, ktorým sa oznámenie zaslalo;

Možné cezhraničné aspekty

16. porušenie ochrany osobných údajov sa týka účastníkov alebo jednotlivcov v iných členských štátoch;
 17. oznámenie zaslané príslušným orgánom iných členských štátov.
-

PRÍLOHA II

Obsah oznámenia určeného účastníkovi alebo jednotlivcovi

1. meno/názov poskytovateľa;
 2. údaje o totožnosti a kontaktné údaje úradníka pre ochranu údajov alebo iné kontaktné miesto, kde možno získať viac informácií;
 3. zhrnutie udalosti, ktorá spôsobila porušenie ochrany osobných údajov;
 4. odhadovaný dátum udalosti;
 5. povaha a obsah dotknutých osobných údajov podľa článku 3 ods. 2;
 6. pravdepodobné dôsledky porušenia bezpečnosti osobných údajov pre dotknutého účastníka alebo jednotlivca podľa článku 3 ods. 2;
 7. okolnosti porušenia ochrany osobných údajov podľa článku 3 ods. 2;
 8. opatrenia, ktoré poskytovateľ prijal na vyriešenie porušenia ochrany osobných údajov;
 9. opatrenia, ktoré poskytovateľ odporúča na zmiernenie možných nepriaznivých účinkov.
-