ROZPORZĄDZENIA

ROZPORZĄDZENIE KOMISJI (UE) NR 611/2013

z dnia 24 czerwca 2013 r.

w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) ([1]), w szczególności jej art. 4 ust. 5,

po konsultacji z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji (ENISA),

po konsultacji z Grupą Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołaną w art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([2]) (Grupa Robocza Art. 29),

po konsultacji z Europejskim Inspektorem Ochrony Danych (EIOD),

a także mając na uwadze, co następuje:

(1) W dyrektywie 2002/58/WE przewiduje się harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu w Unii tego typu danych oraz urządzeń i usług łączności elektronicznej.

(2) Na mocy art. 4 dyrektywy 2002/58/WE dostawcy publicznie dostępnych usług łączności elektronicznej zobowiązani są powiadamiać o przypadkach naruszenia danych osobowych właściwe organy krajowe, a w niektórych okolicznościach również abonentów lub osoby fizyczne, których to dotyczy. Naruszenie danych osobowych zdefiniowano w art. 2 lit. i) dyrektywy 2002/58/WE jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub w inny sposób przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej w Unii.

(3) W celu zapewnienia spójności we wdrażaniu środków, o których mowa w art. 4 ust. 2, 3 i 4 dyrektywy 2002/58/WE, w art. 4 ust. 5 tej dyrektywy uprawniono Komisję do przyjęcia technicznych środków wykonawczych dotyczących okoliczności, formy i trybu mających zastosowanie do wymogów dotyczących informowania i powiadamiania, o których mowa w tym artykule.

(4) Rozbieżne wymogi krajowe w tym zakresie mogą prowadzić do braku pewności prawa, bardziej skomplikowanych i uciążliwych procedur oraz znacznych kosztów administracyjnych dla dostawców transgranicznych. Komisja uznaje zatem, że przyjęcie takich technicznych środków wykonawczych jest niezbędne.

(5) Niniejsze rozporządzenie ogranicza się do powiadamiania o przypadkach naruszenia danych osobowych i nie określa technicznych środków wykonawczych związanych z art. 4 ust. 2 dyrektywy 2002/58/WE, w którym mowa jest o informowaniu abonentów w przypadku szczególnego ryzyka naruszenia bezpieczeństwa sieci.

(6) Z art. 4 ust. 3 akapit pierwszy dyrektywy 2002/58/WE wynika, że dostawca powinien powiadomić właściwy organ krajowy o każdym przypadku naruszenia danych osobowych. Decyzja, czy powiadomić właściwy organ krajowy, nie powinna zatem w żadnym zakresie leżeć w gestii dostawcy. Właściwy organ krajowy powinien mieć jednak możliwość priorytetowego traktowania niektórych badanych przypadków naruszenia według swojego uznania i zgodnie z obowiązującym prawem; powinien on również móc podejmować odpowiednie kroki, aby nie zgłaszano naruszenia, gdy nie ma takiej potrzeby, oraz by nie pomijano żadnych rzeczywistych przypadków naruszenia.

(7) Należy ustanowić system powiadamiania właściwego organu krajowego o przypadkach naruszenia danych osobowych, który to system składa się, jeśli spełnione są określone warunki, z różnych etapów podlegających określonym terminom. System ten ma zapewnić, by właściwy organ krajowy był powiadamiany w najwcześniejszym możliwym terminie i w najbardziej wyczerpujący sposób; system ten nie powinien jednak niepotrzebnie utrudniać dostawcy badania przypadku naruszenia oraz stosowania środków niezbędnych dla jego ograniczenia i zaradzenia jego skutkom.

([1]) Dz.U. L 201 z 31.7.2002, s. 37.
([2]) Dz.U. L 281 z 23.11.1995, s. 31.

(8) Ani samo podejrzenie, że doszło do naruszenia danych osobowych, ani samo wykrycie zdarzenia bez wystarczających dostępnych informacji, mimo starannego działania dostawcy w tym zakresie, nie wystarczą, by uznać, że wykryto naruszenie danych osobowych do celów niniejszego rozporządzenia. Szczególny nacisk należy zatem położyć na dostępność informacji, o których mowa w załącznikach.

(9) W kontekście stosowania niniejszego rozporządzenia właściwe organy krajowe, których to dotyczy, powinny współpracować w przypadkach naruszenia danych osobowych o charakterze transgranicznym.

(10) Niniejsze rozporządzenie nie zawiera dodatkowych szczegółowych przepisów dotyczących rejestru naruszeń danych osobowych, który dostawcy zobowiązani są prowadzić, gdyż zawartość rejestru została wyczerpująco określona w art. 4 dyrektywy 2002/58/WE. Dostawcy mogą jednak odnieść się do niniejszego rozporządzenia przy określaniu formy rejestru.

(11) Wszystkie właściwe organy krajowe powinny udostępnić dostawcom bezpieczne środki elektroniczne służące do powiadamiania w jednolitej formie o przypadkach naruszenia danych osobowych, w oparciu o standardy takie jak XML, zawierające informacje określone w załączniku I w stosownych językach, tak aby wszyscy dostawcy w Unii mogli działać w podobnym trybie niezależnie od tego, gdzie mają swoją siedzibę i gdzie doszło do naruszenia danych osobowych. W związku z powyższym Komisja powinna ułatwić wdrożenie takich bezpiecznych środków elektronicznych, w razie potrzeby organizując spotkania z właściwymi organami krajowymi.

(12) Przy ocenie, czy naruszenie danych osobowych może pociągnąć za sobą niekorzystne skutki dla danych osobowych lub prywatności abonenta lub osoby fizycznej, należy w szczególności uwzględnić charakter i treść przedmiotowych danych osobowych, zwłaszcza w przypadku, gdy dane dotyczą informacji finansowych, takich jak informacje związane z kartą kredytową i rachunkiem bankowym; szczególne kategorie danych, o których mowa w art. 8 ust. 1 dyrektywy 95/46/WE; oraz niektóre dane szczególnie związane ze świadczeniem usług telefonicznych lub internetowych, np. dane dotyczące poczty elektronicznej, dane dotyczące lokalizacji, internetowe pliki rejestru, rejestry przeszukiwanych stron internetowych i wykazy wykonanych usług telekomunikacyjnych.

(13) W wyjątkowych okolicznościach dostawca powinien mieć możliwość powiadomienia abonenta lub osoby fizycznej w późniejszym terminie, jeśli powiadomienie abonenta lub osoby fizycznej może zaszkodzić należytemu zbadaniu przypadku naruszenia danych osobowych. W tym kontekście do wyjątkowych okoliczności można zaliczyć dochodzenie w sprawach karnych oraz inne przypadki naruszenia danych osobowych, które nie stanowią poważnego przestępstwa, ale w odniesieniu do których stosowne może być opóźnienie powiadomienia. W każdym razie do właściwego organu krajowego należy ocena, czy w danym przypadku i w świetle danych okoliczności należy zgodzić się na opóźnienie, czy zażądać powiadomienia.

(14) Dostawcy, ze względu na bezpośredni stosunek umowny, powinni dysponować danymi kontaktowymi swoich abonentów, takie informacje mogą jednak nie być dostępne w odniesieniu do innych osób fizycznych, wobec których naruszenie danych osobowych miało niekorzystne skutki. W takim przypadku należy zezwolić dostawcy na wstępne powiadomienie tych osób fizycznych poprzez ogłoszenia w głównych krajowych lub regionalnych mediach, takich jak gazety, po którym to powiadomieniu wstępnym jak najszybciej powinno nastąpić indywidualne powiadomienie zgodnie z niniejszym rozporządzeniem. Dostawca nie jest zatem zobowiązany do powiadamiania za pośrednictwem mediów, ale jest do tego upoważniony, jeśli uzna to za stosowne podczas identyfikacji wszystkich osób fizycznych, których dotyczyło naruszenie.

(15) Informacja o naruszeniu powinna dotyczyć naruszenia i nie może być powiązana z informacjami na inny temat. Na przykład zawarcie informacji o naruszeniu danych osobowych w zwykłej fakturze należy uznać za niewłaściwy sposób powiadomienia o naruszeniu danych osobowych.

(16) Niniejsze rozporządzenie nie określa szczegółowych technologicznych środków ochrony, które uzasadniają odstępstwo od obowiązku powiadamiania abonentów lub osób fizycznych o przypadkach naruszenia danych osobowych, gdyż środki te zmieniają się w miarę postępu technologicznego. Komisja powinna jednak być w stanie publikować orientacyjny wykaz takich szczegółowych technologicznych środków ochrony zgodnych z bieżącą praktyką.

(17) Samego stosowania szyfrowania czy haszowania nie powinno uważać się za wystarczające, by dostawcy mogli szerzej twierdzić, iż spełnili ogólne wymogi bezpieczeństwa określone w art. 17 dyrektywy 95/46/WE. W tym kontekście dostawcy powinni również wprowadzić odpowiednie środki organizacyjne i techniczne, aby zapobiegać przypadkom naruszenia, wykrywać je i blokować. Dostawcy powinni wziąć pod uwagę wszelkie ewentualne ryzyko szczątkowe istniejące po wprowadzeniu w życie kontroli celem zrozumienia, w jakich sytuacjach może dojść do naruszenia danych osobowych.

(18) Jeżeli dostawca powierza innemu dostawcy wykonanie części usługi, np. w związku z naliczaniem opłat czy zarządzaniem, taki inny dostawca, którego z użytkownikiem końcowym nie łączy bezpośredni stosunek

umowny, nie powinien być zobowiązany do wydawania powiadomień w przypadku naruszenia danych osobowych. Powinien natomiast powiadomić dostawcę, z którym łączy go bezpośredni stosunek umowny. Powyższą procedurę należy również stosować w kontekście hurtowego świadczenia usług łączności elektronicznej, gdzie hurtowego dostawcy z użytkownikiem końcowym nie łączy zazwyczaj bezpośredni stosunek umowny.

(19) W dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych określono ogólne ramy ochrony danych osobowych w Unii Europejskiej. Komisja przedstawiła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady mającego zastąpić dyrektywę 95/46/WE (rozporządzenie o ochronie danych). Proponowanym rozporządzeniem o ochronie danych nałożono by na wszystkich administratorów danych obowiązek powiadamiania o przypadkach naruszenia danych osobowych, biorąc za podstawę art. 4 ust. 3 dyrektywy 2002/58/WE. Niniejsze rozporządzenie Komisji jest w pełni spójne ze wspomnianym proponowanym środkiem.

(20) Proponowane rozporządzenie o ochronie danych wprowadza również pewne techniczne dostosowania w dyrektywie 2002/58/WE w celu uwzględnienia przekształcenia dyrektywy 95/46/WE w rozporządzenie. Skutki materialno-prawne nowego rozporządzenia w odniesieniu do dyrektywy 2002/58/WE będą przedmiotem przeglądu Komisji.

(21) Stosowanie niniejszego rozporządzenia należy poddać przeglądowi trzy lata po jego wejściu w życie, a jego treść należy poddać przeglądowi w świetle obowiązujących w tym czasie ram prawnych, w tym proponowanego rozporządzenia o ochronie danych. Przegląd niniejszego rozporządzenia powinien być w miarę możliwości połączony z przyszłym przeglądem dyrektywy 2002/58/WE.

(22) Stosowanie niniejszego rozporządzenia można ocenić m.in. w oparciu o prowadzone przez właściwe organy krajowe statystyki dotyczące przypadków naruszenia danych osobowych, o których zostały powiadomione. Statystyki te mogą obejmować np. liczbę przypadków naruszenia danych osobowych, o których powiadomiono właściwy organ krajowy, liczbę przypadków naruszenia danych osobowych, o których powiadomiono abonenta lub osobę fizyczną, czas potrzebny na zaradzenie naruszeniu danych osobowych oraz to, czy wprowadzono technologiczne środki ochrony. Statystyki te powinny być dla Komisji i państw członkowskich źródłem spójnych i porównywalnych danych statystycznych i nie powinny ujawniać tożsamości powiadamiającego dostawcy ani tożsamości abonentów ani osób fizycznych, których dotyczy naruszenie. W tym celu Komisja może również odbywać regularne spotkania z właściwymi organami krajowymi i innymi zainteresowanymi podmiotami.

(23) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią Komitetu ds. Łączności,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zakres

Niniejsze rozporządzenie stosuje się do powiadamiania przez dostawców publicznie dostępnych usług łączności elektronicznej (zwanych dalej „dostawcą") o naruszeniu danych osobowych.

Artykuł 2

Powiadomienie właściwego organu krajowego

1. Dostawca powiadamia właściwy organ krajowy o wszystkich przypadkach naruszenia danych osobowych.

2. Dostawca powiadamia właściwy organ krajowy o przypadku naruszenia danych osobowych nie później niż 24 godziny po wykryciu naruszenia danych osobowych, jeśli jest to wykonalne.

W powiadomieniu skierowanym do właściwego organu krajowego dostawca zawiera informacje określone w załączniku I.

Uznaje się, że doszło do wykrycia naruszenia danych osobowych, gdy dostawca uzyskał wystarczającą wiedzę o zaistnieniu zdarzenia naruszającego ochronę, które doprowadziło do naruszenia danych osobowych, w celu przekazania zasadne powiadomienia zgodnie z wymogami niniejszego powiadomienia.

3. Jeśli nie wszystkie informacje określone w załączniku I są dostępne i konieczne jest dalsze badanie przypadku naruszenia danych osobowych, zezwala się dostawcy na wstępne powiadomienie właściwego organu krajowego nie później niż 24 godziny po wykryciu naruszenia danych osobowych. Takie wstępne powiadomienie właściwego organu krajowego zawiera informacje określone w załączniku I sekcja 1. Dostawca przedkłada właściwemu organowi krajowemu drugie powiadomienie najszybciej, jak to możliwe i najpóźniej w ciągu trzech dni po wstępnym powiadomieniu. Takie drugie powiadomienie zawiera informacje określone w załączniku I sekcja 2 oraz w stosownych przypadkach uaktualnienie wcześniej przekazanych informacji.

Jeżeli dostawca, mimo zbadania przypadku, nie jest w stanie przedstawić wszystkich informacji w terminie trzech dni od wstępnego powiadomienia, przedstawia we wspomnianym terminie te informacje, którymi dysponuje, oraz przedkłada właściwemu organowi krajowemu uzasadnienie opóźnienia w przekazaniu pozostałych informacji. Dostawca jak najszybciej przekazuje pozostałe informacje właściwemu organowi krajowemu oraz w stosownych przypadkach jak najszybciej aktualizuje wcześniej przekazane informacje.

4. Właściwy organ krajowy zapewnia wszystkim dostawcom posiadającym siedzibę w państwie członkowskim, którego to dotyczy, bezpieczne środki elektroniczne służące do powiadamiania o przypadkach naruszenia danych osobowych oraz informacje dotyczące trybu dostępu do tych środków i ich stosowania. W stosownych przypadkach Komisja organizuje spotkania z właściwymi organami krajowymi w celu ułatwienia stosowania niniejszego przepisu.

5. Jeżeli naruszenie danych osobowych ma wpływ na abonentów lub osoby fizyczne z państw członkowskich innych niż państwo właściwego organu krajowego, który powiadomiono o naruszeniu danych osobowych, organ ten informuje inne zainteresowane organy krajowe.

Aby ułatwić stosowanie niniejszego przepisu, Komisja tworzy i utrzymuje wykaz właściwych organów krajowych i odpowiednich punktów kontaktowych.

Artykuł 3

Powiadomienie abonenta lub osoby fizycznej

1. Jeśli istnieje prawdopodobieństwo, że naruszenie danych osobowych wywoła niekorzystne skutki dla danych osobowych lub prywatności abonenta lub osoby fizycznej, dostawca, oprócz powiadomienia, o którym mowa w art. 2, powiadamia również o naruszeniu tego abonenta lub tę osobę fizyczną.

2. Prawdopodobieństwo, że naruszenie danych osobowych może mieć niekorzystne skutki dla danych osobowych lub prywatności abonenta lub osoby fizycznej, ocenia się, biorąc od uwagę w szczególności następujące okoliczności:

a) charakter i treść odnośnych danych osobowych, zwłaszcza jeśli dane te związane są z informacjami finansowymi, szczególnymi kategoriami danych, o których mowa w art. 8 ust. 1 dyrektywy 95/46/WE, danymi dotyczącymi poczty elektronicznej, danymi dotyczącymi lokalizacji, internetowymi plikami rejestru, rejestrami przeszukiwanych stron internetowych i wykazami wykonanych usług telekomunikacyjnych;

b) prawdopodobne konsekwencje naruszenia danych osobowych dla danego abonenta lub osoby fizycznej, szczególnie jeżeli naruszenie mogłoby skutkować kradzieżą lub sfałszowaniem tożsamości, uszkodzeniem ciała, cierpieniem psychicznym, upokorzeniem lub naruszeniem dobrego imienia; oraz

c) okoliczności, w jakich doszło do naruszenia danych osobowych, w szczególności to, gdzie skradziono dane oraz kiedy dostawca dowiedział się, że dane są w posiadaniu nieupoważnionej strony trzeciej.

3. Powiadomienie abonenta lub osoby fizycznej następuje bez zbędnej zwłoki po wykryciu naruszenia danych osobowych, jak określono w art. 2 ust. 2 akapit trzeci. Powyższe nie jest zależne od powiadomienia o naruszeniu danych osobowych skierowanego do właściwego organu krajowego, o którym mowa w art. 2.

4. W powiadomieniu skierowanym do abonenta lub osoby fizycznej dostawca zawiera informacje określone w załączniku II. Powiadomienie skierowane do abonenta lub osoby fizycznej sformułowane jest w sposób jasny i łatwo zrozumiały. Dostawca nie wykorzystuje powiadomienia jako okazji do promowania lub reklamowania nowych lub dodatkowych usług.

5. W wyjątkowych okolicznościach, gdy powiadomienie abonenta lub osoby fizycznej może zaszkodzić należytemu zbadaniu przypadku naruszenia danych osobowych, dostawcy zezwala się, po uprzednim uzyskaniu zgody właściwego organu krajowego, na powiadomienie abonenta lub osoby fizycznej w późniejszym terminie, który właściwy organ krajowy uzna za możliwy do celów powiadomienia o naruszeniu danych osobowych zgodnie z niniejszym artykułem.

6. Dostawca powiadamia abonenta lub osobę fizyczną o naruszeniu danych osobowych, używając środków komunikacji zapewniających szybkie dotarcie informacji i odpowiednio zabezpieczonych zgodnie z najnowszym stanem wiedzy w tej dziedzinie. Informacja o naruszeniu dotyczy naruszenia i nie jest powiązana z informacjami na inny temat.

7. Jeżeli w terminie, o którym mowa w ust. 3, oraz mimo odpowiednich starań, dostawca związany z końcowym użytkownikiem bezpośrednim stosunkiem umownym nie jest w stanie zidentyfikować wszystkich osób fizycznych, wobec których naruszenie danych osobowych prawdopodobnie ma niekorzystne skutki, dostawca może w tymże terminie powiadomić te osoby poprzez ogłoszenia w głównych mediach krajowych lub regionalnych w danych państwach członkowskich. Ogłoszenia te zawierają informacje określone w załączniku II, w razie potrzeby w formie skróconej. W takim przypadku dostawca nadal podejmuje odpowiednie starania, by zidentyfikować te osoby i jak najszybciej przekazać im informacje określone w załączniku II.

Artykuł 4

Technologiczne środki ochrony

1. Na zasadzie odstępstwa od art. 3 ust. 1 powiadomienie danego abonenta lub osoby fizycznej o naruszeniu danych osobowych nie jest wymagane, jeżeli dostawca wykazał w sposób wymagany przez właściwy organ krajowy, że wprowadził w życie odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie bezpieczeństwa. Tego rodzaju technologiczne środki ochrony sprawiają, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.

2. Dane uznaje się za nieczytelne, jeżeli:

a) zostały bezpiecznie zaszyfrowane z użyciem ustandaryzowanego algorytmu, klucz używany do odszyfrowywania tych danych nie został złamany w wyniku naruszenia bezpieczeństwa, oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków; lub

b) zostały zastąpione wartością klucza haszującego, obliczoną za pomocą standaryzowanej kryptograficznej funkcji haszującej z kluczem tajnym, klucz użyty do haszowania tych danych nie został złamany w wyniku naruszenia bezpieczeństwa, oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków.

3. Po konsultacji z właściwymi organami krajowymi w ramach Grupy Roboczej Art. 29, Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji oraz Europejskim Inspektorem Ochrony Danych Komisja może opublikować orientacyjny wykaz stosownych technologicznych środków ochrony, o których mowa w ust. 1, zgodnie z bieżącą praktyką.

Artykuł 5

Korzystanie z usług innego dostawcy

Jeżeli zawarto umowę z innym dostawcą, który będzie świadczyć część usługi łączności elektronicznej i który nie jest związany z abonentami bezpośrednim stosunkiem umownym, dostawca ten niezwłocznie powiadamia dostawcę zamawiającego o przypadku naruszenia danych osobowych.

Artykuł 6

Sprawozdawczość i przegląd

W ciągu trzech lat od wejścia w życie niniejszego rozporządzenia Komisja przedstawi sprawozdanie dotyczące jego stosowania, skuteczności skutków dla dostawców. Na podstawie tego sprawozdania Komisja dokona przeglądu niniejszego rozporządzenia.

Artykuł 7

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie z dniem 25 sierpnia 2013 r., dwa miesiące po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 24 czerwca 2013 r.

W imieniu Komisji
José Manuel BARROSO
Przewodniczący

ZAŁĄCZNIK I

Treść powiadomienia właściwego organu krajowego

Sekcja 1

Identyfikacja dostawcy

1. Nazwa dostawcy

2. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, w którym można uzyskać więcej informacji

3. Informacja o tym, czy jest to pierwsze, czy drugie powiadomienie

Wstępne informacje dotyczące naruszenia danych osobowych (do uzupełnienia w stosownych przypadkach w późniejszych powiadomieniach)

4. Data i godzina zdarzenia (jeśli jest znana; w razie potrzeby można określić w przybliżeniu)

5. Okoliczności naruszenia danych osobowych (np. utrata, kradzież, kopiowanie)

6. Charakter i treść przedmiotowych danych osobowych

7. Środki techniczne i organizacyjne, które zostały lub mają być zastosowane przez dostawcę w odniesieniu do danych osobowych będących przedmiotem naruszenia

8. Istotne w kontekście naruszenia korzystanie z usług innych dostawców (w stosownych przypadkach)

Sekcja 2

Dalsze informacje dotyczące naruszenia danych osobowych

9. Streszczenie zdarzenia, w wyniku którego doszło do naruszenia danych osobowych (w tym określenie miejsca, w którym fizycznie doszło do naruszenia, oraz nośników, których dotyczyło naruszenie)

10. Liczba abonentów lub osób fizycznych, których dotyczy naruszenie

11. Potencjalne konsekwencje i potencjalne niekorzystne skutki dla abonentów lub osób fizycznych

12. Techniczne lub organizacyjne środki wprowadzone przez dostawcę w celu złagodzenia potencjalnych niekorzystnych skutków

Ewentualne dodatkowe powiadomienie abonentów lub osób fizycznych

13. Treść powiadomienia

14. Zastosowane środki komunikacji

15. Liczba powiadomionych abonentów lub osób fizycznych

Ewentualne kwestie transgraniczne

16. Naruszenie danych osobowych dotyczące abonentów lub osób fizycznych w innych państwach członkowskich

17. Powiadomienie innych właściwych organów krajowych

ZAŁĄCZNIK II

Treść powiadomienia abonenta lub osoby fizycznej

1. Nazwa dostawcy

2. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, w którym można uzyskać więcej informacji

3. Streszczenie zdarzenia, w wyniku którego doszło do naruszenia danych osobowych

4. Przybliżona data zdarzenia

5. Charakter i treść przedmiotowych danych osobowych, zgodnie z art. 3 ust. 2

6. Prawdopodobne konsekwencje naruszenia danych osobowych dla danego abonenta lub osoby fizycznej, zgodnie z art. 3 ust. 2

7. Okoliczności naruszenia danych osobowych, zgodnie z art. 3 ust. 2

8. Środki wprowadzone przez dostawcę w celu zaradzenia naruszeniu ochrony danych osobowych

9. Środki zalecane przez dostawcę w celu złagodzenia ewentualnych niekorzystnych skutków