01119/13/PL

WP197

Opinia 6/2012 na temat projektu decyzji Komisji w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej[1]

Przyjęta 12 lipca 2012 r.

[1] Opinia odnosi się do decyzji Komisji („projekt decyzji Komisji w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej"), która z przyczyn technicznych przyjęła formę rozporządzenia („rozporządzenie w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej").

Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europesjkiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH

W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 ust. 1 lit. a) i ust. 3 powyższej dyrektywy,

uwzględniając swój regulamin,

PRZYJMUJE NINIEJSZĄ OPINIĘ

1 Wprowadzenie i zakres projektu decyzji

Na mocy art. 4 ust. 5 dyrektywy 2002/58/WE, zmienionej dyrektywą 2009/136/WE (zwanej dalej „*dyrektywą o prywatności i łączności elektronicznej*"), Komisja Europejska (zwana dalej „*Komisją*") może przyjąć środki wykonawcze dotyczące art. 4 ust. 2, 3 i 4 tej dyrektywy, po konsultacji z właściwymi zainteresowanymi stronami, w tym z grupą roboczą powołaną na mocy art. 29 (zwaną dalej „*grupą roboczą*").

Jak podkreślono w szczególności w motywie 5, projekt decyzji Komisji (zwanej dalej „decyzją") obejmuje jedynie ust. 3 i 4, które dotyczą przypadków naruszenia danych osobowych. Powyższe wskazuje na to, że kwestia *szczególnego ryzyka naruszenia bezpieczeństwa sieci* zostanie podjęta w osobnej decyzji Komisji. Decyzja powinna zostać rozpatrzona również w świetle projektu rozporządzenia w sprawie ochrony danych[2], który proponuje rozszerzenie powiadamiania o przypadkach naruszenia danych osobowych na wszystkich administratorów danych.

W tym względzie grupa robocza z zadowoleniem przyjmuje decyzję, która przyczyni się do harmonizacji praktycznych zasad związanych z powiadamianiem o przypadkach naruszenia danych osobowych.

W niniejszej opinii grupa robocza pragnie jednak zwrócić uwagę Komisji na niektóre zagadnienia poruszone w decyzji, które wymagają wyjaśnienia i udoskonalenia.

2 Analiza

2.1 Terminologia i pewność prawa

Grupa robocza z zadowoleniem przyjmuje fakt, że Komisja włożyła duży wysiłek w wyjaśnienie przepisów dyrektywy dotyczących przypadków naruszenia danych osobowych.

---

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF

Równocześnie jednak grupa robocza jest zaniepokojona częstym posługiwaniem się nieprecyzyjnymi sformułowaniami, takimi jak „dostateczna" lub „wyjątkowe okoliczności", które może prowadzić do różnych interpretacji oraz braku pewności prawa i w konsekwencji negatywnie wpłynąć na wszystkie zainteresowane podmioty.

a) terminy „dostateczną" i „odpowiednio"

Artykuł 2 ust. 2 stanowi, że „*W przypadku naruszenia danych osobowych dostawca powiadamia właściwy organ krajowy o przypadku naruszenia danych osobowych nie później niż 24 godziny po tym, jak uzyska* **dostateczną pewność***, że zaistniało naruszenie danych osobowych*". W celu uniknięcia niepewności w ustaleniu momentu, od którego rozpocznie się 24 godzinny okres zwłoki grupa robocza proponuje uproszczenie tego zdania w następując sposób „*W przypadku naruszenia danych osobowych dostawca powiadamia właściwy organ krajowy o przypadku naruszenia danych osobowych nie później niż 24 godziny po wykryciu naruszenia danych osobowych*".

Poza tym grupa robocza zauważa, że w decyzji nie uwzględniono w sposób wyraźny przypadków, w których dostawca wykrywa zdarzenie naruszające bezpieczeństwo danych osobowych, które może doprowadzić lub mogło doprowadzić do naruszenia danych osobowych, nie będąc jednak w stanie ustalić, czy zdarzenie w istocie doprowadziło do naruszenia danych osobowych. W decyzji można by podkreślić, że dostawca winien zdawać sobie sprawę z tego, że wykryte zdarzenie naruszające bezpieczeństwo danych osobowych, które mogłoby podlegać rozwiązaniu w oparciu o najlepsze praktyki branżowe z zakresu zarządzania zdarzeniami naruszającymi bezpieczeństwo danych osobowych, może w istocie prowadzić do naruszenia danych osobowych; dostawca powinien być zatem przygotowany do przeprowadzenia oceny i podjęcia działania.

W art. 2 ust. 3 również użyto terminów „dostateczną/odpowiednich":

- podobnie jak wyżej, fragment „*zezwala się dostawcy na wstępne powiadomienie właściwego organu krajowego nie później niż 24 godziny po tym, jak uzyska* **dostateczną pewność***, że zaistniało naruszenie danych osobowych*" można by zmienić w następujący sposób „*zezwala się dostawcy na wstępne powiadomienie właściwego organu krajowego nie później niż 24 godziny po wykryciu naruszenia danych osobowych*",

- fragment „*mimo podjęcia* **odpowiednich starań** *w celu zbadania przypadku*" można by zastąpić – bez utraty przejrzystości – fragmentem „*mimo zbadania przypadku*". W każdym razie to właściwy organ będzie ostatecznie dokonywał analizy argumentów przedstawionych przez dostawcę, uzasadniających jakąkolwiek zwłokę w powiadomieniu.

W art. 3 ust. 8 również występuje termin „odpowiednich/odpowiednie": „*Jeżeli w terminie, o którym mowa w ust. 3, oraz mimo* **odpowiednich starań***, dostawca nie jest w stanie zidentyfikować wszystkich osób fizycznych, wobec których naruszenie danych osobowych ma niekorzystne skutki, dostawca może w tymże terminie powiadomić te osoby o niemożliwości przeprowadzenia identyfikacji poprzez ogłoszenia w głównych mediach krajowych.*

Ogłoszenia te zawierają informacje określone w załączniku II, w razie potrzeby w formie skróconej. Ponadto w takim przypadku dostawca nadal podejmuje **odpowiednie starania**, *by zidentyfikować te osoby i jak najszybciej przekazać im informacje określone w załączniku II*." Grupa robocza proponuje uprościć analizowany ustęp w drodze usunięcia odniesień do terminu „odpowiednich starań" w następujący sposób: „*Jeżeli w terminie, o którym mowa w ust. 3, dostawca nie jest w stanie zidentyfikować wszystkich osób fizycznych, wobec których naruszenie danych osobowych ma niekorzystne skutki, dostawca może w tymże terminie powiadomić te osoby o niemożliwości przeprowadzenia identyfikacji poprzez ogłoszenia w głównych mediach krajowych. Ogłoszenia te zawierają informacje określone w załączniku II, w razie potrzeby w formie skróconej. Ponadto w takim przypadku dostawca nadal podejmuje starania, by zidentyfikować te osoby i jak najszybciej przekazać im informacje określone w załączniku II."*

W motywie 6 oraz w art. 3 ust. 3 powinno unikać się terminu „*odpowiedni*".

W art. 3 ust. 7 wskazuje się ponadto, że „*dostawca powiadamia abonenta lub osobę fizyczną o naruszeniu danych osobowych, używając* **odpowiednio** *zabezpieczonych środków komunikacji zapewniających szybkie dotarcie informacji*". Grupa robocza proponuje zmianę ostatniej części zdania w następujący sposób „*używając środków komunikacji zapewniających szybkie dotarcie informacji i odpowiednio zabezpieczonych*[3] *zgodnie z najnowszym stanem wiedzy w tej dziedzinie*".

b) wyrażenie „wyjątkowe okoliczności"

Wyrażenie „*wyjątkowe okoliczności*" powoduje taką samą niepewność. Grupa robocza zauważa, że wyrażenie „wyjątkowe okoliczności" może już być zdefiniowane w ustawodawstwie krajowym lub orzecznictwie, odnosząc się na przykład do „*nieprzewidywalnych zdarzeń o szczególnie poważnym charakterze*", włączając w jego zakres wojny lub poważne zdarzenia związane z bezpieczeństwem publicznym. Taka interpretacja wydaje się niezgodna z celami decyzji, którymi są harmonizacja i doprecyzowanie.

W związku z powyższym grupa robocza zaleca, aby doprecyzować tekst decyzji w następujący sposób:

1) w art. 2 ust. 3 ostatni akapit fragment „**W wyjątkowych okolicznościach***, jeżeli dostawca, mimo* **podjęcia odpowiednich starań w celu zbadania przypadku** *[...]"* zastąpić fragmentem *„jeżeli dostawca, mimo zbadania przypadku[...]*".

W celu zachowania spójności podobny zwrot powinien zostać użyty w motywie 6.

Ponadto grupa robocza zaleca, aby w decyzji zawarto wyraźne odniesienie do art. 15a dyrektywy o prywatności i łączności elektronicznej celem podkreślenia, że brak lub niepełne

[3] „zabezpieczony" oznacza „zapewniający poufność, integralność i dostępność".

powiadomienie o przypadku naruszenia danych osobowych może stanowić pogwałcenie przepisów dotyczących naruszenia danych osobowych.

2) w art. 3 ust. 6 decyzji stanowi się, że „*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 odpowiednim terminie późniejszym.*" Grupa robocza z zadowoleniem przyjmuje fakt, że powiadomienie właściwego organu co do zasady nie następuje ze zwłoką, doskonale również rozumie, że w pewnych okolicznościach może zaistnieć potrzeba opóźnienia powiadomienia osób fizycznych przykładowo celem uniknięcia zakłócenia dochodzenia prowadzonego przez policję. Jednakże użycie wyrażenia „wyjątkowe okoliczności" skutkuje brakiem pewności prawa co do zakresu takiego wyłączenia, może również dawać dostawcom szerokie pole manewru do opóźniania powiadomień skierowanych do osób fizycznych. Grupa robocza zwraca się zatem do Komisji, by wyraźnie określiła zakres „wyjątkowych okoliczności", o których mowa w tekście[4]. W tym względzie – mając na uwadze równowagę między uzasadnionym interesem dochodzenia prowadzonego przez policję i obowiązkiem informowania osób fizycznych w przypadkach, w których wspomniane informacje mogą z dużą dozą pewności przyczynić się do złagodzenia ewentualnych negatywnych skutków naruszenia – priorytetem powinna być zawsze ochrona osób fizycznych.

c) uwagi dodatkowe

Pierwsze zdanie motywu 6 rozpoczyna się w następujący sposób: „*Dostawcy* **powinni** *powiadomić właściwy organ* [...]". Grupa robocza proponuje użycie konstrukcji „powiadamiają" zamiast „powinni powiadomić", w tym przypadku w celu zachowania spójności z dyrektywą, jak również z art. 2 ust. 1 decyzji.

Ponadto grupa robocza proponuje skreślić art. 3 ust. 5 decyzji, ponieważ nie wprowadza on dodatkowych informacji, zaleceń lub wymogów w stosunku do postanowień już istniejących w dyrektywie oraz w art. 3 ust. 1 decyzji.

2.2 Powiadomienie właściwego organu krajowego

Zgodnie z art. 4 ust. 3 dyrektywy o prywatności i łączności elektronicznej „*W przypadku naruszenia danych osobowych, dostawca publicznie dostępnych usług łączności elektronicznej bez zbędnej zwłoki powiadamia o tym przypadku naruszenia danych osobowych właściwy organ krajowy.*"

---

[4] Przykładowo Komisja – jeżeli pragnie w sposób wyraźny odnieść się do poważnych przypadków z zakresu dochodzeń prowadzonych przez policję – może powołać się na brzmienie art. 1 dyrektywy 2006/24/WE, który odnosi się w szczególności do „*celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego*". Komisja może przyjąć inne brzmienie przepisu, jeżeli „wyjątkowe okoliczności" mają odnosić się w bardziej szczegółowy sposób do przestępczości komputerowej.

Decyzja rozwija pojęcie „*zbędnej zwłoki*” poprzez wprowadzenie dwóch rodzajów opóźnienia: pierwsze opóźnienie w wymiarze 24 godzin po wykryciu naruszenia celem przedstawienia „wstępnego powiadomienia” z podstawowymi informacjami oraz drugie opóźnienie w wymiarze trzech dni po wstępnym powiadomieniu celem dostarczenia w pełni uzupełnionego powiadomienia. W załączniku 1 do decyzji szczegółowo wymieniono minimalną zawartość treści wstępnego powiadomienia (sekcja 1) i powiadomienia uzupełnionego (sekcja 2).

Z zastrzeżeniem uprzednio podkreślonych uwag dotyczących zastosowania terminu „odpowiedni”, grupa robocza z zadowoleniem przyjmuje fakt umieszczenia w decyzji dwóch rodzajów szczególnych opóźnień, popiera również dwuetapowy system powiadamiania umożliwiający połączenie zdolności reagowania i kompleksowości.

Grupa robocza proponuje kilka zmian w celu ułatwienia komunikacji między dostawcą i organem oraz w celu zapewnienia lepszej harmonizacji[5].

a) informacje, które powinny być przedstawione i wstępne powiadomienie

Absolutne minimum informacji, które dostawca musi zgłosić właściwemu organowi w przeciągu 24 godzin od wykrycia naruszenia, ogranicza się do nazwy dostawcy i nazwy punktu kontaktowego (załącznik I sekcja 1). W takiej formie, bez dodatkowych informacji, wstępne powiadomienie przedstawia niewielką wartość dla właściwego organu. Grupa robocza uważa, że w celu zachęcenia dostawców do wprowadzania wysokiej jakości polityki bezpieczeństwa danych osobowych, dostawca winien być zobligowany do przedstawienia właściwemu organowi krajowemu większej ilości informacji aniżeli proponuje Komisja. Zdaniem grupy roboczej dostawca powinien powiadomić właściwy organ o wszystkich szczegółach, o których ma wiedzę, podczas pierwszego etapu powiadamiania. W ramach wstępnego powiadomienia obowiązkowe powinno być zamieszczenie przynajmniej pewnej ograniczonej liczby dodatkowych pozycji. Grupa robocza uważa, że w przypadku, gdy dostawca wykrył naruszenie, winien mieć on świadomość przynajmniej rodzaju danych osobowych, których dotyczy zdarzenie, okoliczności naruszenia lub rodzaju naruszenia (utrata, kradzież, kopiowanie itp.), a także sposobu wykrycia naruszenia (znajdujące się na miejscu oprogramowanie służące wykrywaniu naruszeń, analiza rejestrów, zgłoszenie zdarzenia przez pracownika itp.). Wskazane informacje powinny być uwzględnione we wstępnym powiadomieniu, a następnie uzupełnione lub skorygowane w powiadomieniu drugim.

---

[5] W trakcie opracowywania projektów przyszłych przepisów dotyczących naruszeń danych osobowych Komisja mogłaby także zastanowić się, czy o wszystkich naruszeniach danych osobowych należy powiadamiać właściwe organy, czy też można byłoby zastosować w niektórych przypadkach wyłączenia od tej zasady, pod warunkiem że wszelkie naruszenia podlegałyby odnotowaniu w rejestrze prowadzonym przez administratora danych. Kwestia ta została już poruszona przez grupę roboczą w opinii 1/2009 na temat wniosków zmieniających dyrektywę 2002/58/WE o prywatności i łączności elektronicznej.

Grupa robocza proponuje dodanie następujących informacji w sekcji 1 załącznika I do decyzji:

- okoliczności naruszenia danych osobowych/rodzaj naruszenia (np. utrata, kradzież, kopiowanie)
- sposób wykrycia naruszenia
- data i godzina wykrycia zdarzenia, a także data i godzina, w której miało miejsce zdarzenie
- charakter i treść przedmiotowych danych osobowych
- przeprowadzone kontrole (w szczególności w odniesieniu do nieczytelności danych osobowych)

Decyzja powinna również wyraźnie wskazywać na to, że dostawca może zmienić elementy wstępnego powiadomienia w uzupełnionym drugim powiadomieniu.

Wreszcie, w celu umożliwienia konstruowania odesłań do pozycji powiadomienia wymienionych w załączniku I, grupa robocza proponuje zastąpienie punktów numerami. Jest to również przydatne w kontekście rozwoju zharmonizowanego podejścia w przypadku wykorzystania środków elektronicznych służących do powiadamiania.

b) środki elektroniczne

Wykorzystanie środków elektronicznych do przekazywania powiadomień wydaje się właściwym rozwiązaniem i grupa robocza popiera inicjatywę Komisji Europejskiej zmierzającą do promowania – w miarę możliwości – takich środków. Jednakże wdrożenie środków elektronicznych w poszczególnych państwach członkowskich nie nastąpi w sposób natychmiastowy: konieczne będzie zdefiniowanie wspólnego elektronicznego formatu powiadamiania, przyjęcie właściwych środków bezpieczeństwa, stworzenie i przetestowanie środków elektronicznych (portal lub inny system typu zabezpieczona wiadomość elektroniczna), których celem będzie wzmocnienie tego typu procedury w każdym państwie członkowskim.

W związku z powyższym decyzja powinna przewidywać opracowanie, we współpracy z odpowiednimi zainteresowanymi stronami, prostego i jednolitego europejskiego elektronicznego formatu powiadamiania (np. XML). Z chwilą, gdy taki jednolity format zostanie określony, Komisja Europejska powinna zezwolić na co najmniej 12-miesięczne opóźnienie w celu wdrożenia systemu powiadamiania drogą elektroniczną. Podczas trwania okresu przejściowego dopuszczone powinny być alternatywne sposoby powiadamiania.

Grupa robocza zwraca się do Komisji z prośbą o wskazanie, czy i w jaki sposób Komisja zapewni wsparcie finansowe i logistyczne w kontekście ewentualnego projektu grupy roboczej i poszczególnych organów ds. ochrony danych mającego na celu określenie jednolitego formatu oraz wdrożenie rozwiązań technicznych dla potrzeb powiadamiania o

przypadkach naruszenia przez administratorów danych organów ds. ochrony danych, jak również wymianę między właściwymi organami wszelkich informacji dotyczących przypadków naruszenia danych w sprawach transgranicznych. Projekt ten powinien również uwzględniać rozwiązania, które zostały już wdrożone lub które są opracowywane w niektórych państwach członkowskich.

c) powiadomienie innych zainteresowanych organów krajowych

W art. 2 ust. 5 decyzji ustanawia się wymóg powiadomienia innych zainteresowanych organów krajowych „*jeżeli naruszenie danych osobowych obejmuje abonentów lub osoby fizyczne z państw członkowskich innych niż państwo właściwego organu krajowego, który powiadomiono o naruszeniu danych osobowych*".

Grupa robocza z zadowoleniem przyjmuje i popiera aktywną współpracę między organami ds. ochrony danych, jak również doskonale rozumie potrzebę jej występowania pomiędzy właściwymi organami krajowymi. Członkowie grupy roboczej wykazują duże zaangażowanie na rzecz wzajemnej współpracy w tym zakresie.

Jednakże obowiązek ten nie istnieje w dyrektywie, w związku z tym grupa robocza zastanawia się nad podstawą prawną takiego obowiązku i praktycznymi skutkami w przypadku braku powiadomienia innych organów krajowych. Ponadto grupa robocza zauważa, że formularz powiadomienia zawarty w załączniku I nie pozwala właściwym organom krajowym na określenie lokalizacji lub narodowości osób, których dotyczy naruszenie, decyzja natomiast nie zapewnia jasnej definicji „abonentów lub osób fizycznych z innych państw członkowskich".

W związku z powyższym grupa robocza zaleca Komisji, by określiła zakres przepisu ustanowionego w art. 2 ust. 5 i wyjaśniła praktyczne środki, jakie celem współpracy winny stosować właściwe organy.

2.3 Powiadomienie abonenta lub osoby fizycznej

Grupa robocza za korzystny uznaje fakt, że w decyzji przedstawiono procedurę dla przypadków, w których nie jest możliwy bezpośredni dostęp do osób, których dotyczy naruszenie.

Grupa robocza przyjmuje również z zadowoleniem – wskazany w art. 3 ust. 2 decyzji – opis okoliczności, które należy uwzględnić przy ocenie, czy naruszenie wywoła niekorzystne skutki dla danych osobowych lub prywatności abonenta lub osoby fizycznej.

W art. 3 ust. 7 podkreśla się, że zawarcie „informacji o naruszeniu danych osobowych w zwykłej fakturze" nie jest właściwym sposobem przekazania informacji osobom fizycznym. Jednakże nie jest jasne, czy jest to tylko przykład, czy też w decyzji zamierza się zakazać stosowania faktur celem przekazania osobom fizycznym informacji o naruszeniu danych osobowych. Ujmując to bardziej ogólnie, grupa robocza jest zdania, że informacje o naruszeniu danych osobowych należy odróżnić od innych informacji wymienianych między

dostawcami i osobami fizycznymi. Grupa robocza proponuje w związku z tym, aby w decyzji zaznaczono, że informacja o naruszeniu powinna dotyczyć naruszenia i nie może być powiązana z informacjami na inny temat.

W odniesieniu do wykorzystania mediów celem dotarcia do osób fizycznych, których dostawca nie jest w stanie zidentyfikować, grupa robocza podkreśla, że mogą zdarzyć się przypadki, w których główne media krajowe nie będą najbardziej odpowiednie, np. w sytuacji, gdy lokalny dostawca będzie chciał dotrzeć do osób fizycznych w obrębie ograniczonego obszaru geograficznego. Aby odzwierciedlić taką ewentualność, w art. 3 ust. 8 po wyrażeniu „poprzez ogłoszenia w głównych mediach krajowych" można dodać wyrazy „lub regionalnych".

Wreszcie, jak zostało to wyjaśnione poniżej, powinno zapewnić się bardziej szczegółowe wytyczne mające pomóc organom ds. ochrony danych oraz dostawcom w dokonaniu oceny stopnia dotkliwości naruszenia w sposób obiektywny i zharmonizowany.

2.4 Ocena stopnia dotkliwości i negatywnych skutków

Wraz z wdrożeniem dyrektywy 2009/136/WE właściwe organy otrzymują coraz więcej powiadomień o przypadkach naruszenia danych osobowych, które różnią się znacznie pod względem zakresu i stopnia dotkliwości. Dla organów ważne jest, aby identyfikowały najpoważniejsze naruszenia w celu nadania priorytetowego znaczenia ich działaniom, które w szczególności obejmują w pewnych okolicznościach ewentualność zmuszenia dostawców do powiadomienia osób fizycznych. Ponadto także dostawcy muszą w sposób wyraźny i obiektywny oszacować niekorzystne skutki naruszenia celem ustalenia, czy powiadamianie osób fizycznych pozostaje uzasadnione.

W związku z powyższym grupa robocza wskazuje na potrzebę opracowania jednolitej oraz łatwej do zrozumienia metody oceny stopnia dotkliwości naruszenia, zarówno dla dostawców, jak i właściwych organów w Europie. W istocie, w art. 3 ust. 2 nie proponuje się ani skali, ani obiektywnych kryteriów w celu oceny wagi stopnia dotkliwości naruszenia. Ponadto wskazany przepis nie podaje żadnych progów, które można by wziąć pod uwagę w celu określenia obowiązku powiadomienia przez dostawcę osób fizycznych.

Treść decyzji zyskałaby na wprowadzeniu w tym zakresie bardziej szczegółowych wytycznych. W istocie, zarówno właściwe organy, jak i dostawcy muszą wypracować jednolitą interpretację i ocenę dotkliwości naruszenia danych osobowych. Kwestia ta jest istotna nie tylko na szczeblu krajowym, lecz również na poziomie europejskim w celu uniknięcia niebezpieczeństwa rozdrobnienia w trakcie wdrażania dyrektywy i decyzji.

W celu wyeliminowania tego niebezpieczeństwa grupa robocza stanowczo popiera ustanowienie, w oparciu o obiektywne kryteria, zharmonizowanej paneuropejskiej metody oceny stopnia dotkliwości naruszenia. Grupa robocza, we współpracy z Europejską Agencją

ds. Bezpieczeństwa Sieci i Informacji, prowadzi obecnie prace nad opracowaniem takiej metody[6]. Proponowana metoda wprowadzi skalę dotkliwości naruszenia, która będzie brała pod uwagę niekorzystne skutki dla osób fizycznych, wysiłek niezbędny do identyfikacji osób fizycznych na podstawie danych oraz poziom narażenia danych, których dotyczy naruszenie. Jednakże zwłaszcza liczba osób fizycznych, których dotyczy naruszenie, nie powinna być wykorzystywana jako kryterium w celu określenia, czy powiadomienie tych osób jest wymagane. Grupa robocza zaleca Komisji, aby zapewniła, że zharmonizowane podejście do oceny stopnia dotkliwości naruszenia będzie wykorzystywane przez wszystkie zainteresowane strony. Opracowanie ram oceny dotkliwości naruszenia powinno być zatem bezpośrednio uwzględnione w specjalnym artykule decyzji.

Ponadto grupa robocza proponuje, aby decyzja obejmowała w ramach obszarów koniecznych zawartych w sekcji 2 załącznika I zarówno odpowiednie kryteria wykorzystane w ocenie stopnia dotkliwości naruszenia, jak również wynik oceny wagi stopnia dotkliwości naruszenia (np. waga „wysoka", „średnia", „niska" lub „nieistotna"), a także uzasadnienie takiej oceny.

2.5 Technologiczne środki ochrony oraz nieczytelność danych

W art. 4 decyzji określa się w sposób bardziej szczegółowy, jakie środki uważa się za wystarczające, by sprawić, że dane stają się nieczytelne. Środki te, które w głównej mierze oparte są na zaleceniach Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, uwypuklają fakt, że aby można było uznać dane za nieczytelne, musi to nastąpić w wyniku zastosowania mechanizmu szyfrującego, funkcji haszującej z kluczem tajnym albo w wyniku nieodwracalnego usunięcia. Środki te wskazują również na to, że powiązane klucze kryptograficzne nie mogą być łatwe do odszyfrowania oraz że nie mogły one zostać złamane w wyniku ewentualnych przypadków naruszenia zasad bezpieczeństwa. Grupa robocza uznaje takie środki za korzystne, jest również zdania, że będą one stanowić zachętę dla zainteresowanych stron do tworzenia bardziej rygorystycznych praktyk w zakresie bezpieczeństwa, przy jednoczesnym zapewnieniu większej pewności prawa w odniesieniu do pojęcia danych nieczytelnych w poszczególnych państwach członkowskich.

W przypadku gdy naruszenie danych osobowych dotyczy wyłącznie danych, które stały się nieczytelne, powoduje to, że dostawca – zgodnie z prawem – może zostać zwolniony z wymogu powiadamiania osób fizycznych w przypadku naruszenia danych osobowych. Niemniej jednak grupa robocza pragnie podkreślić, że decyzja, o której mowa, nie powinna prowadzić do tego, aby podmioty gospodarcze odniosły wrażenie, że samo stosowanie szyfrowania, haszowania czy bezpiecznego usuwania jest wystarczające, by dostawcy mogli 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.

---

[6] W oparciu o „zalecenia w sprawie technicznych wytycznych dotyczących wdrożenia art. 4" opracowane przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji.

W tym celu dostawcy muszą na miejscu posiadać ramowy system zarządzania ryzykiem[7], tak by móc określić odpowiednie środki, jakie powinny zostać wdrożone. Ważne jest również, aby dostawcy wzięli pod uwagę wszelkie ewentualne ryzyko szczątkowe istniejące po wprowadzeniu w życie kontroli celem zrozumienia, w jakich potencjalnych sytuacjach może dojść do przypadków naruszenia danych osobowych. Grupa robocza zaleca Komisji wyjaśnienie tej kwestii w motywie decyzji.

W odniesieniu do definicji „*danych nieczytelnych*" grupa robocza, celem uniknięcia niejasności, pragnie zaproponować pewne niewielkie zmiany do tekstu decyzji poprzez rozbicie ust. 2 lit. a) na dwie części, tak by lepiej rozróżnić szyfrowanie i haszowanie, w następujący sposób:

> *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; lub*
>
> *c) zostały nieodwracalnie usunięte poprzez fizyczne zniszczenie nośnika, na którym je zapisano, lub za pomocą algorytmu bezpiecznego usuwania danych.*

Proponowane rozróżnienie między szyfrowaniem i haszowaniem pozwala na podkreślenie następujących istotnych punktów, które w obecnym tekście decyzji mogą nie być do końca jasne:

1) bezpieczeństwo szyfrowania w większym stopniu zależy od bezpieczeństwa klucza „odkodowującego" niż klucza „kodującego"; pomimo że wskazane rozróżnienie nie dotyczy algorytmów symetrycznych (takich jak AES), ma ono znaczenie w przypadku szyfrowania asymetrycznego (takiego jak RSA),
2) bezpieczeństwo funkcji haszującej z kluczem tajnym opiera się na kluczu użytym do obliczenia funkcji haszującej i nie istnieje pojęcie klucza „odkodowującego" lub klucza „kodującego",

[7] System ramowy powinien koncentrować się na ochronie danych osobowych oraz powinien identyfikować potencjalny wpływ na osoby fizyczne, w przeciwieństwie do koncentrowania się wyłącznie na zagrożeniach dotyczących działalności gospodarczej, powinien również skupiać się na ochronie organizacji w kontekście ryzyka prawnego.

3) w przypadku haszowania warto wyjaśnić, że pierwotne dane zostały „zastąpione" wartością klucza haszującego (tak jak na przykład w bazach danych haseł) i że wartość klucza haszującego nie jest powiązana z innymi bezpośrednimi lub pośrednimi danymi identyfikacyjnymi,
4) ważne jest, aby uściślić, że właściwe klucze są zastrzeżone dla osób, które są „*nieupoważnione do poznania klucza*"; w związku z tym rozszyfrowanie klucza w drodze wyczerpującego wyszukiwania klucza nie powinno być możliwe dla „*osób nieupoważnionych do poznania klucza*", zgodnie z tym, co zostało dodane w tekście.

Ponadto w odniesieniu do koncepcji usunięcia proponuje się zastąpić fragment „*bezpiecznie usunięte*" wyrażeniem „*nieodwracalnie usunięte*" w celu doprecyzowania zamierzonych rezultatów omawianego środka.

2.6 Pozostałe uwagi

Grupa robocza zauważa, że projekt decyzji nie zawiera żadnego przepisu lub motywu dotyczącego rejestru, o którym mowa w art. 4 ust. 4 dyrektywy. Biorąc pod uwagę ścisły związek między powiadomieniami i rejestrem, grupa robocza proponuje dodanie w decyzji motywu, tak aby wskazać, że dostawcy w celu określenia formatu wpisów zamieszczanych w rejestrze mogą również odnieść się do decyzji.

Podobnie, projekt decyzji Komisji wskazuje w motywie 11, że właściwe organy prowadzą statystyki dotyczące przypadków naruszeń. Grupa robocza proponuje, aby decyzja zawierała zharmonizowany zbiór elementów – które mogłyby być wyodrębnione z jednolitego formularza – celem prowadzenia w sposób statystyczny monitoringu.

Sporządzono w Brukseli dnia 12 lipca 2012 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM