693/14/PL
WP 213

Opinia 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych

Przyjęta w dniu 25 marca 2014 r.

Streszczenie

W niniejszej opinii Grupa Robocza Art. 29 przedstawia wytyczne dla administratorów danych, aby pomóc im w podejmowaniu decyzji w sprawie powiadomienia osób, których dane dotyczą, w razie „naruszenia danych osobowych”. Chociaż niniejsza opinia dotyczy istniejącego obowiązku dostawców usług łączności elektronicznej, wynikającego z dyrektywy 2002/58/WE, zawiera ona jednak przykłady z wielu sektorów w kontekście projektu rozporządzenia o ochronie danych oraz opis dobrych praktyk adresowany do wszystkich administratorów danych.

O ile w dyrektywie 2002/58/WE wymaga się powiadamiania właściwego organu o wszystkich naruszeniach danych osobowych, w niniejszej opinii przeprowadzono analizę naruszeń danych osobowych wymagających powiadomienia osób, których dane dotyczą, oraz przedstawiono działania, które administratorzy danych mogli podjąć podczas wdrażania systemu w celu uniknięcia przedmiotowego naruszenia danych osobowych, lub co najmniej środki, które można było wdrożyć w celu zwolnienia administratora danych z obowiązku powiadomienia osób, których dane dotyczą.

W opinii udzielono ponadto odpowiedzi na niektóre z podstawowych pytań dotyczących naruszeń danych osobowych i stosowania dyrektywy 2002/58/WE.

1. Wprowadzenie

W art. 2 lit. i) dyrektywy 2002/58/WE „naruszenie danych osobowych" zostało zdefiniowane 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 we Wspólnocie".

W dyrektywie 2002/58/WE (oraz we wniosku dotyczącym europejskiego rozporządzenia o ochronie danych) wymaga się powiadamiania właściwego organu krajowego o przypadkach naruszenia danych osobowych. Jeżeli chodzi o takie powiadomienie, w załączniku I do rozporządzenia nr 611/2013 udostępniono szczegółowe informacje, które należy przedstawić.

W przypadku gdy naruszenie danych osobowych może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność osoby, której dane dotyczą[1], administrator danych bez zbędnej zwłoki powiadamia również o takim naruszeniu osobę, której dane dotyczą[2].

W dyrektywie 2002/58/WE oraz w rozporządzeniu nr 611/2013 zawarto odstępstwo od wymogu powiadamiania osób, których dane dotyczą, jeżeli dane stają się nieczytelne. Powiadomienie danej osoby, której dane dotyczą, o naruszeniu danych osobowych nie jest wymagane, jeżeli dostawca wykazał w sposób wymagany przez właściwy organ, że wdrożył odpowiednie technologiczne środki ochrony, aby dane stały się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich[3], oraz jeżeli środki te zostały zastosowane do danych, których dotyczyło naruszenie danych osobowych[4].

Powodem przedmiotowego zwolnienia z obowiązku powiadamiania osób fizycznych jest fakt, że odpowiednie środki mogą ograniczyć szczątkowe ryzyko naruszenia prywatności osób, których dane dotyczą, do nieistotnego poziomu. Naruszenie poufności danych osobowych, które zaszyfrowano przy użyciu najnowocześniejszego algorytmu, nadal stanowi naruszenie danych osobowych i musi zostać zgłoszone właściwemu organowi. Jeżeli jednak nie dojdzie do naruszenia poufności klucza, to dane zasadniczo pozostają nieczytelne dla każdej nieuprawnionej osoby i nie jest prawdopodobne, aby takie naruszenie wywarło niekorzystny wpływ na osobę, której dane dotyczą, a zatem nie zachodzi konieczność powiadomienia o nim takiej osoby.

Nawet jeżeli dane są zaszyfrowane, ich utrata lub zmiana może jednak wywrzeć niekorzystny wpływ na osoby, których dane dotyczą, jeżeli administrator danych nie posiada odpowiednich

[1] W niniejszej opinii termin „osoba, której dane dotyczą" stosujemy w rozumieniu definicji podanej w dyrektywie 95/46/WE. W kontekście dyrektywy 2002/58/WE termin ten odpowiada terminowi „abonent lub osoba fizyczna".

[2] Zgodnie z dyrektywą 2002/58/WE i rozporządzeniem nr 611/2013 właściwy organ zostaje powiadomiony nie później niż 24 godziny po wykryciu naruszenia danych osobowych, jeśli jest to wykonalne. W niektórych przypadkach termin ten można przedłużyć do 72 godzin. Powiadomienie abonenta lub osoby fizycznej następuje bez zbędnej zwłoki (w rozumieniu art. 2 ust. 2 rozporządzenia nr 611/2013) po wykryciu naruszenia danych osobowych. Powiadomienie osoby, której dane dotyczą, nie jest zależne od powiadomienia skierowanego do właściwego organu krajowego.

[3] Dyrektywa 2002/58/WE, art. 4 ust. 3; rozporządzenie nr 611/2013, art. 4 ust. 1; ogólne rozporządzenie o ochronie danych, przedstawiona przez sprawozdawcę nieoficjalna wersja skonsolidowana przegłosowana przez Komisję LIBE, art. 32 ust. 3.

[4] Należy zauważyć, że, jeżeli klucz został w ostatnim czasie złamany, wówczas wszystkie naruszenia dokonane w przeszłości, które nie zostały zgłoszone na podstawie poufności klucza, będą musiały zostać zgłoszone.

kopii zapasowych. W takim przypadku powiadomienie osób, których dane dotyczą, nadal powinno być wymagane, nawet jeżeli zastosowano środki ochrony za pomocą szyfrowania.

W związku z tym ważne jest, aby administratorzy danych byli proaktywni i odpowiednio planowali. Artykuł 17 dyrektywy 95/46/WE, oraz art. 4 ust. 1 i 1 lit. a) dyrektywy 2002/58/WE, stanowi, że administratorzy danych muszą podejmować odpowiednie środki techniczne i organizacyjne, aby zapewnić „poziom bezpieczeństwa odpowiedni do zagrożeń" wynikających z przetwarzania danych. W tym celu ważne jest, aby istniały wdrożone odpowiednie ramy zarządzania ryzykiem, obejmujące minimalną liczbę elementów, które powinno zawierać tego rodzaju podejście, oraz zapewniające zestaw minimalnych, odpowiednich kontroli technicznych i organizacyjnych, które mogą zostać zdefiniowane przez administratora danych, przy czym szczególną wagę należy przykładać do kontroli zapewniających brak czytelności danych, jeżeli zajdzie taka potrzeba. Przedsiębiorstwa powinny również zawczasu określić odpowiednie plany postępowania w przypadkach naruszeń danych osobowych, zapewniające ich szybką i skuteczną reakcję w przypadku naruszenia danych osobowych.

W przypadku prawidłowego zastosowania się do art. 17, tj. przed rozpoczęciem przetwarzania danych, ryzyko związane z naruszeniem danych osobowych zostaje zawczasu uwzględnione i ograniczone. W takich przypadkach przypadki naruszeń danych osobowych mogą zdarzać się rzadziej i z mniej poważnymi konsekwencjami dla osób, których dane dotyczą. Ponieważ powiadamianie osób, których dane dotyczą, nie jest wymagane, jeżeli naruszenie nie wywiera niekorzystnego wpływu na dane osobowe lub prywatność osób, których dane dotyczą, lub jeżeli w stosunku do danych, których dotyczy naruszenie, zastosowano odpowiednie technologiczne środki ochrony, najlepszym sposobem na uniknięcie konieczności powiadomienia osób, których dane dotyczą, jest uwzględnienie odpowiednich zabezpieczeń prywatności w projektach obejmujących przetwarzanie danych.

Powiadamianie osób, których dane dotyczą, powinno odbywać się bez zbędnej zwłoki[5] i nie powinno być uzależnione od powiadomienia właściwego organu krajowego o danym przypadku naruszenia danych osobowych. Administrator danych powinien pamiętać, że jedną z głównych korzyści wynikających z powiadomienia osób fizycznych, nawet jeżeli nie stanowi ona kryterium przy podejmowaniu decyzji w sprawie powiadomienia, jest udzielenie osobom, których dane dotyczą, informacji niezbędnych do ograniczenia niekorzystnych skutków wynikających z okoliczności naruszenia. Jeżeli administrator danych ma wątpliwości dotyczące prawdopodobieństwa wystąpienia niekorzystnego wpływu na dane osobowe lub prywatność osoby, której dane dotyczą, powinien wykazać się przesadną ostrożnością i powiadomić daną osobę. Należy również uwzględnić możliwość żądania przez właściwe organy powiadomienia osób fizycznych w następstwie dalszej oceny powiadomienia.

Opinia zawiera **niepełny wykaz przykładów sytuacji, w których należy powiadamiać osoby, których dane dotyczą**[6]. W niniejszej opinii każdy przypadek naruszenia danych osobowych analizuje się w oparciu o trzy klasyczne kryteria bezpieczeństwa: termin

[5] Zgodnie z dyrektywą 2002/58/WE i rozporządzeniem nr 611/2013 właściwy organ zostaje powiadomiony nie później niż 24 godziny po wykryciu naruszenia danych osobowych, jeśli jest to wykonalne. W niektórych przypadkach termin ten można przedłużyć do 72 godzin. Powiadomienie abonenta lub osoby fizycznej następuje bez zbędnej zwłoki po wykryciu naruszenia danych osobowych.

[6] Ponieważ we wniosku dotyczącym rozporządzenia o ochronie danych przewiduje się objęcie obowiązkiem powiadamiania wszystkich sektorów, a w szeregu państw członkowskich już obecnie obowiązuje prawny obowiązek powiadamiania, przykłady podane w niniejszej opinii nie ograniczają się do sektora łączności elektronicznej.

„naruszenie dotyczące dostępności danych” będzie zatem odpowiadać przypadkowemu lub bezprawnemu zniszczeniu lub utracie danych osobowych, „naruszenie dotyczące integralności danych” będzie dotyczyć zmiany danych osobowych, natomiast „naruszenie dotyczące poufności danych” będzie dotyczyć nieuprawnionego ujawnienia danych osobowych lub dostępu do nich. Następna część opinii zawiera **ogólne wytyczne** dotyczące przypadków niewymagających powiadamiania. W ostatniej części **omówione zostały główne problemy**, z jakimi mogą mieć do czynienia administratorzy danych stając przed dylematem, czy należy powiadomić osoby, których dane dotyczą, czy też nie.

2. Naruszenia, które mogą wywierać niekorzystny wpływ na osoby, których dane dotyczą

Osoby, których dane dotyczą, powinny być bezzwłocznie powiadomione o naruszeniach, które mogą wywierać niekorzystny wpływ na dane osobowe lub prywatność. W niniejszej części przedstawia się przykłady naruszeń spełniających przedmiotowe kryteria. Podano tu również przykłady środków technicznych, dzięki którym można byłoby uniknąć powiadomienia osób, których dane dotyczą, gdyby zostały one wdrożone, zanim doszło do naruszenia.

Przypadek 1. *Z instytutu zdrowia dziecka skradziono cztery laptopy, w których przechowywano szczególnie chronione dane dotyczące zdrowia i opieki społecznej oraz inne dane dotyczące 2 050 dzieci.*

Przedmiotowe naruszenie danych osobowych dotyczy poufności oraz (jeżeli administrator danych nie dysponował żadnymi kopiami zapasowymi danych) dostępności i integralności danych.

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- pierwszym skutkiem jest naruszenie tajemnicy lekarskiej: baza danych zawiera osobiste informacje medyczne dotyczące dzieci, do których dostęp uzyskały osoby nieupoważnione;
- publikacja takich danych może wywrzeć wpływ na otoczenie szkolne lub rodzinne dziecka (np. dane dotyczące napaści, chorób przewlekłych, problemów psychicznych, trudności społecznych lub finansowych rodziny itp.);
- naruszenie może spowodować negatywne skutki emocjonalne u dzieci i ich rodziców;
- takie dane mogą zostać wykorzystane w celu szantażowania rodziców i dzieci (w zależności od ich wieku);
- rodzice nieuleczalnie chorych dzieci mogą paść ofiarą osób (takich jak oszuści, członkowie sekt itp.) pragnących czerpać zyski z ich cierpienia.

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego dostępności danych:

- naruszenie może zakłócić ciągłość leczenia dzieci, prowadząc do pogłębienia lub nawrotu choroby;
- naruszenie może prowadzić do przypadkowego zatrucia organizmu w wyniku reakcji alergicznej na lek lub leki, których nie należy łączyć, co może doprowadzić do różnych problemów zdrowotnych lub śmierci;
- naruszenie może skutkować zbędną zwłoką w refundacji lub pomocy finansowej na rzecz osób, których dane dotyczą, co wywarłoby wpływ finansowy na rodziny dzieci.

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego integralności danych:

- utracone dane mogą wpłynąć na integralność dokumentacji medycznej i spowodować przerwę w leczeniu dzieci. Przykładowo, jeżeli istnieje jedynie stara kopia zapasowa dokumentacji medycznej, wszystkie zmiany danych dokonane w skradzionych komputerach zostaną utracone, skutkując zakłóceniem integralności danych. Korzystanie z nieaktualnej dokumentacji medycznej może spowodować przerwanie ciągłości leczenia dzieci, prowadząc do pogłębienia lub nawrotu choroby.

Ze względu na potencjalne skutki należy w tym przypadku powiadomić o naruszeniu danych osobowych, przy czym ważne jest również jednak, aby uwzględnić wiek i dojrzałość osób, których dane dotyczą. Lepszym rozwiązaniem może być powiadomienie rodzica lub opiekuna prawnego, który aktywnie uczestniczy w opiece medycznej nad dzieckiem, oprócz powiadomienia samych dzieci, jeżeli jest to odpowiednie lub wymagane w przepisach prawnych mających zastosowanie.

Powiadomieni rodzice będą w stanie zgłosić nieprawidłowość w ciągłości leczenia, sprawdzić alergie znane instytutowi lub poprosić o wykonanie nowych badań lekarskich, aby mieć pewność, że ich dzieci są odpowiednio leczone. Będą mogli również zdecydować się na bezpośrednie poinformowanie dodatkowych osób o stanie zdrowia dzieci, aby kontrolować niektóre skutki dla otoczenia dzieci.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- posiadanie wystarczających aktualnych i bezpiecznych kopii zapasowych zapobiegłoby naruszeniu dotyczącemu dostępności i integralności danych, lub ograniczyło jego skutki i niekorzystny wpływ;
- potencjalne skutki i niekorzystny wpływ naruszenia dotyczącego poufności danych można było ograniczyć, chroniąc dane poprzez zastosowanie odpowiedniego produktu szyfrującego wykorzystującego wystarczająco silny i tajny klucz.

Gdyby zastosowano takie zabezpieczenia i zapewniono ich bezpieczeństwo (tj. klucz pozostałby tajny, a kopia zapasowa dostępna), powiadomienie osób fizycznych zasadniczo może nie być konieczne. Należy to wykazać zgodnie z wymogami właściwego organu.

Przypadek 2. *Doszło do bezprawnego dostępu do danych osobowych dotyczących klientów agenta ubezpieczeniowego wskutek wykorzystania podatności aplikacji na atak sieciowy. Osoby, których dane dotyczą, zostały zidentyfikowane z imienia i nazwiska, oraz został podany ich adres zamieszkania oraz pełne kwestionariusze dotyczące stanu zdrowia. Naruszenie objęło 700 osób, których dane dotyczyły.*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- dane opublikowane w internecie przez atakującego mogą mieć wpływ na zdolność osób, których dane dotyczą, do znalezienia pracy (odpowiedzi dotyczące problemów zdrowotnych, ciąży itp.);

- naruszenie może mieć wpływ na otoczenie zawodowe lub rodzinne osób, których dane dotyczą;
- naruszenie może również mieć skutki emocjonalne, jeżeli osoby, których dane dotyczą, ukrywają zdiagnozowaną chorobę;
- naruszenie może prowadzić do oszustwa dotyczącego tożsamości;
- dane (np. fakt bycia klientem lub opłacania określonych usług) mogą zostać wykorzystane do celów wyłudzania informacji (phishingu).

Ponieważ w tym przypadku prawdopodobne jest wystąpienie niekorzystnego wpływu na osobę, których dane dotyczą, należy ją powiadomić o naruszeniu.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- można było zapobiec naruszeniu lub ograniczyć jego skutki, gdyby stale monitorowano potencjalne luki w stosowanych technologiach, w tym gdyby regularnie skanowano strony internetowe pod kątem luk lub aktualizowano oprogramowanie (w tym oprogramowanie zabezpieczające).

  Chociaż trudno jest zapobiec podatności na atak dokonywany za pomocą programów zero-day exploit, margines ryzyka można ograniczyć do dopuszczalnego poziomu za pomocą odpowiednich i skutecznych strategii na rzecz aktywnego zapobiegania wykorzystywaniu podatności na atak, w przeglądu kodu. Ponadto skutkom naruszenia można zapobiec dzięki dobrej polityce zarządzania zdarzeniami naruszającymi ochronę, ograniczając zakres niekorzystnego wpływu naruszenia oraz czas jego występowania;

- podobnie jak w poprzednim przykładzie, potencjalne skutki i niekorzystny wpływ naruszenia dotyczącego poufności danych można było ograniczyć, gdyby chroniono dane dotyczące klientów, stosując odpowiedni produkt szyfrujący wykorzystujący wystarczająco silny i tajny klucz. Może to być szczególnie skuteczny sposób ochrony przed kradzieżą dysku lub w przypadku wystąpienia podobnych okoliczności;

  ponadto zakład ubezpieczeń mógł użyć różnych technologii służących wzmocnieniu ochrony prywatności w celu ograniczenia ilości danych lub identyfikowalności osoby, której dane dotyczą. Przykładowo zakład mógł wysyłać losowy numer identyfikacyjny pocztą, tak aby jego klienci mogli wypełnić kwestionariusz dotyczący stanu zdrowia online. W ten sposób można uniknąć podawania imienia i nazwiska, adresu, daty urodzenia lub numeru telefonu w kwestionariuszu wypełnianym online.

Przypadek 3. *Pracownik dostawcy usług internetowych podał stronie trzeciej login i hasło do konta z prawem ogólnego dostępu do bazy danych klientów. Korzystając z tego konta, strona trzecia może uzyskać dostęp do wszystkich informacji dotyczących klientów bez żadnych ograniczeń. Baza danych zawiera imię i nazwisko, adres, adres email, numery telefonu, dane dostępu i inne dane identyfikujące (nazwa użytkownika, hasła szyfrowane funkcją haszującą, numer identyfikacyjny klienta) oraz dane dotyczące płatności (numer konta, dane karty kredytowej itp.). Mimo że dane dotyczące płatności zaszyfrowano przy użyciu najnowocześniejszego algorytmu, z konta głównego, do którego się włamano, można było uzyskać dostęp do tych danych, a zatem strona trzecia również miała do nich dostęp. Przedsiębiorstwo posiada ponad 100 000 klientów.*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- niewłaściwe wykorzystanie danych dotyczących płatności (zwłaszcza danych kart kredytowych) miałoby finansowe skutki dla klientów;
- ponieważ w odniesieniu do haseł zastosowano jedynie funkcję haszującą, strona trzecia może bez problemu odgadnąć odpowiadający zwykły tekst. Dostęp do

konta każdego klienta byłby możliwy nawet po zamknięciu konta, którego dotyczyło naruszenie;

- strona trzecia mogłaby z łatwością skorzystać z adresu email i hasła niektórych osób, których dane dotyczą i na które ma wpływ naruszenie, w celu uzyskania dostępu do kont innych usług online, ponieważ wiele osób używa tego samego hasła w odniesieniu do wielu różnych usług online.

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego integralności danych:

- strona trzecia miała całkowity dostęp do bazy danych, przez co mogła zmieniać, usuwać lub dodawać określone dane dotyczące konta;
    - jeżeli usługi świadczone przez danego dostawcę usług internetowych obejmowały pocztę elektroniczną lub hosting, strona trzecia mogła mieć dostęp do takich treści, lub mogła je zmienić lub usunąć, lub dokonać zmiany ustawień DNS (ang. *Domain Name System* – system nazw domenowych) lub zamknąć konto osoby, której dane dotyczą.

Chociaż dane finansowe były zaszyfrowane, strona trzecia miała dostęp do odszyfrowanych danych przez interfejs użytkownika, a zatem nie ma tu zastosowania zwolnienie z obowiązku powiadamiania.

Jeżeli zabezpieczone pliki dziennika są wiarygodne (tj. nie doszło do naruszenia ich bezpieczeństwa) i na ich podstawie można stwierdzić, że z danego konta nie wchodzono do bazy danych klientów, wówczas powiadomienie osoby, której dane dotyczą, nie powinno stanowić wymogu.

W każdym innym przypadku, ponieważ w opisanej sytuacji prawdopodobne jest wystąpienie niekorzystnego wpływu na osoby, których dane dotyczą i nie ma zastosowania zwolnienie, klienci, których dotyczy naruszenie, powinni zostać o nim powiadomieni.

Zawsze gdy dochodzi do złamania haseł, do celów bezpieczeństwa administrator danych powinien wymusić w bezpieczny sposób na osobach, których dane dotyczą, utworzenie nowego hasła, zapewniając wprowadzenie wszystkich nowych haseł przez prawowitych użytkowników, a nie przez strony trzecie, które uzyskały dane logowania. W praktyce ta procedura może odpowiadać bezpiecznej procedurze odnowienia straconego hasła oraz powinna obejmować informacje dotyczące podstawowej przyczyny odnowienia hasła. Powiadamiając użytkownika, należy również zalecić mu, aby nie stosował tego samego lub podobnego hasła co poprzednio oraz aby zmienił złamane hasła do wszystkich kont, do których loguje się za pomocą tego samego hasła.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- każdej osobie fizycznej należy przydzielić jej własne konta, a uprawnienia do dostępu do danych osobowych należy przyznawać wyłącznie na zasadach ograniczonego dostępu i minimalnego uprzywilejowania. Ma to również zastosowanie do sprzedawców, personelu obsługi będącego stroną trzecią oraz do innych osób, które tymczasowo potrzebują dostępu do bazy danych: takim osobom należy udzielić dostępu wyłącznie do funkcji i danych, których potrzebują w celu wykonania wyznaczonych im zadań przez okres nie dłuższy niż jest to konieczne do wykonania takich zadań. Stosowanie kont z „ogólnym dostępem” do bazy danych powinno być ograniczone i należy wdrożyć metody śledzenia i ograniczania użycia tego rodzaju kont. Gdyby wprowadzono tego rodzaju zabezpieczenia, można byłoby uniknąć takiego naruszenia lub ograniczyć jego skutki;
- gdyby hasła przechowywano w bezpieczny sposób (tzn. stosując ciąg zaburzający i kryptograficzną funkcję haszującą), w dużym stopniu uniknięto by wtórnego negatywnego wpływu na osoby fizyczne. Na ryzyko nadal mogą być jednak

narażone osoby fizyczne posługujące się słabym hasłem, zwłaszcza gdy wykorzystują te same dane uwierzytelniające w odniesieniu do innych usług online. Przedmiotowe ryzyko można byłoby ograniczyć, sugerując takim użytkownikom stosowanie silniejszych haseł.

Przypadek 4. *Koperta zawierająca dowody zakupu kartą płatniczą lub kredytową przez pomyłkę została wyrzucona do kosza na śmieci i nie została zniszczona w bezpieczny sposób. Zawartość kosza na śmieci została przerzucona do dużego pojemnika ustawionego na zewnątrz budynku na potrzeby zbiórki odpadów. Jakaś osoba fizyczna wyjęła kopertę z drugiego pojemnika, a następnie rozpowszechniła zawarte w niej dowody dokonania zakupu kartą płatniczą lub kredytową na okolicznym osiedlu mieszkaniowym. Dane obejmowały pełne dane dotyczące kart*[7] *oraz imię i nazwisko właściciela karty. W niektórych przypadkach dostępne były również podpisy właściciela karty. Naruszenie objęło 800 osób, których dane dotyczą.*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- naruszenie mogłoby wywrzeć wpływ finansowy na osoby, których dane dotyczą, jeżeli dane dotyczące ich kart są nadal ważne i zostaną niewłaściwie użyte[8].

Ponieważ w tym przypadku prawdopodobne jest wystąpienie niekorzystnego wpływu na osoby, których dane dotyczą, takie osoby należy powiadomić o naruszeniu. W opisanej sytuacji, jeżeli nie przechowywano żadnych innych danych, powiadomienie każdej osoby, której dane dotyczą, z osobna wydaje się trudne, ponieważ może nie być wiadome, które konkretnie dowody zakupu kartą płatniczą lub kredytową znajdowały się w kopercie. Sklep powinien powiadomić podmiot obsługujący płatności dokonywane kartami, aby mógł on monitorować potencjalnie nielegalne transakcje. Inne praktyczne rozwiązanie zaproponowano w rozporządzeniu nr 611/2013[9], które stanowi, że „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 prawdopodobnie ma niekorzystne skutki, dostawca może w tymże terminie powiadomić te osoby poprzez ogłoszenia w głównych mediach krajowych lub regionalnych w danych państwach członkowskich". W związku z tym w przypadku sklepu, którego klientami są głównie lokalni mieszkańcy, powiadomienie w formie ogłoszenia w regionalnej gazecie można uznać za wystarczające. Ponadto powiadomienie operatorów kart kredytowych o naruszeniu może pomóc chronić ich klientów.

Jeżeli administrator danych odzyskałby nieotwartą kopertę z któregoś z pojemników, zdarzenie prawdopodobnie nie wywarłoby niekorzystnego wpływu na właścicieli kart, a zatem osoby, których dane dotyczą i nie zaistniałaby konieczność powiadamiania ich o naruszeniu.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

[7] Chociaż najlepszą praktyką jest ucinanie danych dotyczących płatności dokonywanych kartą na drukowanym paragonie klienta, to jednak funkcja ta nie jest dostępna we wszystkich terminalach płatniczych i na kopiach paragonów sprzedawcy mogą być drukowane pełne dane.

[8] Ponieważ dane dotyczące kart można wykorzystać nawet bez znajomości kodu CVV (lub równoważnego zabezpieczenia), należy powiadamiać nawet o naruszeniach, które nie dotyczą kodu CVV.

[9] Chociaż w tym kontekście rozporządzenie to nie ma zastosowania.

- informowanie pracowników o możliwych skutkach takich naruszeń oraz korzystanie z odpowiednich biurowych niszczarek dokumentów10 lub usługi niszczenia archiwum w celu zniszczenia dowodów dokonania zakupu kartą płatniczą lub kredytową (i wszystkich podobnych dokumentów papierowych zawierających dane osobowe) przed ich wyrzuceniem w znacznym stopniu ograniczyłoby ryzyko wystąpienia tego rodzaju naruszenia;
- korzystanie z terminala płatniczego, który nie obejmuje pełnych danych karty kredytowej.

[10] Na przykład niszczarka dokumentów klasy 2 zapewniająca poziom bezpieczeństwa P-4 lub wyższy wg klasyfikacji DIN 66399 dla dokumentów papierowych.

Przypadek 5. *Z bagażnika samochodu został skradziony laptop, którego zawartość została zaszyfrowana, należący do doradcy finansowego. Zdarzenie ma wpływ na wszystkie dane dotyczące ocen finansowych – obejmujące przykładowo kredyty hipoteczne, wynagrodzenia, wnioski o udzielenie pożyczki – odnoszące się do 1 000 osób, których dane dotyczą. Chociaż nie doszło do złamania klucza szyfrowania ani hasła, to jednak nie jest dostępna żadna kopia zapasowa.*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- w zależności od dokładnego charakteru danych, których dotyczy naruszenie, niewłaściwe zastosowanie danych może wywierać różny wpływ na osoby, których dane dotyczą. Ponieważ jednak w laptopie zastosowano pełne szyfrowanie dysku (za pomocą najnowocześniejszej technologii), a dostępu chroni silne hasło, które nie zostało złamane, nie doszło do nieuprawnionego ujawnienia danych.

Potencjalne konsekwencje i niekorzystny wpływ:

- brak dostępu do danych wymaga ponownego podania niezbędnych informacji przez osoby, których dane dotyczą. Oznacza to zatem wywarcie nieznacznego negatywnego skutku na osoby, których dane dotyczą, w postaci konieczności wykonania czasochłonnych czynności oraz irytacji;
- w niektórych przypadkach może oznaczać to niedotrzymanie terminów przedłożenia dokumentów lub wniosków, co może powodować różnego rodzaju wtórne skutki doświadczane przez osoby, których dane dotyczą, w zależności od sytuacji: grzywny, uszczuplenie dochodów lub oczekiwanych zysków, utratę możliwości, zerwanie umowy kupna itp.

Ponieważ dane zostały utracone, a skutki naruszenia dotyczącego dostępności danych nie zostały ograniczone, naruszenie danych osobowych prawdopodobnie wywrze niekorzystny wpływ na osobę, której dane dotyczą. Dlatego też o naruszeniu należy poinformować osoby, których dane dotyczą i na które ma wpływ naruszenie. W powiadomieniu należy nie tylko wyjaśnić, że konieczne będzie ponowne przekazanie informacji doradcy finansowemu, lecz także należy poinformować osoby, których dane dotyczą, o różnych ewentualnych konsekwencjach i niekorzystnych skutkach, z którymi mogą się spotkać w związku z naruszeniem.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- skuteczne i bezpieczne rozwiązanie w zakresie kopii zapasowych umożliwiłoby odzyskanie danych. Jeżeli dostępne byłyby aktualne kopie zapasowe danych, nie doszłoby do naruszenia dotyczącego dostępności danych, a zatem powiadamiania o naruszeniu nie byłoby konieczne.

Przypadek 6. *Operator sieci ruchomej zapewnia możliwość prowadzenia konta online, za pośrednictwem którego, po zalogowaniu, abonenci mają wgląd w ostatnie rachunki i działalność na koncie. Okazało się, że doszło do nielegalnego dostępu do bazy danych, w której przechowuje się hasła do strony internetowej. Strona trzecia uzyskała dostęp do danych uwierzytelniania użytkowników (nazwa użytkownika i hasła zaszyfrowane algorytmem MD-5 bez zastosowania ciągu zaburzającego).*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- strona trzecia może odgadnąć hasło, a zatem uzyskać dostęp do konta każdego klienta, ponieważ dysponuje też nazwami użytkowników;
- ponieważ wiele osób stosuje to samo połączenie nazwy użytkownika i hasła do wielu kont online, strona trzecia prawdopodobnie może uzyskać dostęp do innych kont niektórych osób, których dane dotyczą i na które ma wpływ naruszenie, w tym w określonych przypadkach do kont poczty elektronicznej.

Ponieważ w odniesieniu do haseł zastosowano jedynie funkcję haszującą, nie można ich uznać za nieczytelne, zgodnie z definicją podaną w art. 4 ust. 2 rozporządzenia Komisji nr 611/2013[11]. W związku z powyższym nie ma tu zastosowania zwolnienie z obowiązku powiadamiania osób, których dane dotyczą.

Ponieważ w opisanej sytuacji prawdopodobne jest wystąpienie niekorzystnego wpływu na osoby, których dane dotyczą, i nie ma zastosowania zwolnienie, klientów, których dotyczy naruszenie, należy o tym powiadomić oraz należy wyraźnie zalecić użytkownikom zmianę ich haseł do wszystkich kont opatrzonych tym samym, złamanym hasłem. W każdym razie należy zażądać od wszystkich użytkowników zmiany ich haseł – z zastosowaniem bezpiecznej metody – przy próbie dostępu do przedmiotowej usługi.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- gdyby hasła przechowywano w bezpieczny sposób (tj. hasła z ciągiem zaburzającym i szyfrowane kryptograficzną funkcją haszującą przy zastosowaniu najnowocześniejszej funkcji haszującej i klucza lub ciągu zaburzającego), w znacznym stopniu ograniczono by niekorzystny wpływ na osoby fizyczne. Na ryzyko nadal mogą jednak być narażone osoby fizyczne stosujące słabe hasło, zwłaszcza gdy wykorzystują te same dane dostępu w odniesieniu do innych usług online.

[11] Artykuł 4 ust. 2 stanowi, że:

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.

Przypadek 7. *Dostawca usług internetowych zapewnia abonentom możliwość wglądu w informacje dotyczące ich konta, historię korzystania z internetu, w tym miesięczną przepustowość i często odwiedzane domeny. Błąd kodowania na stronie internetowej spowodował brak uwierzytelnienia danych dostępu użytkownika oraz możliwość dostępu do danych w wyniku manipulacji wartością ID abonenta umieszczoną w parametrach URL. Możliwe jest uzyskanie dostępu do informacji dotyczących kont wszystkich klientów za pomocą przeglądania kolejnych ID abonenta.*

Potencjalne konsekwencje i niekorzystny wpływ naruszenia dotyczącego poufności danych:

- dane mogą być wykorzystywane do rozsyłania spamu do osób, których dane dotyczą, na adresy email lub numery telefonu;
- dane mogą posłużyć do tworzenia profilu abonenta i ujawnienia szczegółów jego zachowania, które mogą spowodować ujawnienie danych szczególnie chronionych. Naruszenie może mieć wpływ na otoczenie zawodowe lub rodzinne osób, których dane dotyczą.

Naruszenie może mieć niekorzystny wpływ na daną osobę fizyczną, dlatego też klienci powinni zostać o nim powiadomieni.

Przykładowe odpowiednie zabezpieczenia, dzięki którym można byłoby ograniczyć ryzyko, gdyby zostały one zawczasu wdrożone:

- możliwe, że naruszenia można byłoby uniknąć, gdyby monitorowano potencjalne luki w stosowanych technologiach, co opisano w przykładzie 2, oraz przeprowadzono przedprodukcyjne testy platformy przed jej uruchomieniem, a także przeprowadzano przegląd kodu.

3. Ewentualne sytuacje, w których powiadomienie osób, których dane dotyczą, nie jest wymagane

Chociaż oceny skutków naruszenia danych osobowych należy dokonywać w poszczególnych przypadkach, w celu należytego uwzględnienia wszystkich elementów oceny prawdopodobnego niekorzystnego wpływu na osoby fizyczne administrator danych może również uznać, do celów ogólnych wytycznych i uzupełnienia zwolnień opisanych w powyższej części, że powiadomienie osób, których dane dotyczą, nie jest konieczne w niektórych określonych przypadkach.

Takie przypadki mogą obejmować:

- naruszenie danych osobowych dotyczące jedynie poufności danych, jeżeli dane zostały bezpiecznie zaszyfrowane z użyciem najnowocześniejszego 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. W praktyce tego rodzaju środki sprawiają, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich;

- w stosunku do danych, takich jak hasła, zastosowanie bezpiecznej funkcji skrótu i ciągu zaburzającego. Dane zostały zastąpione wartością klucza haszującego, obliczoną za pomocą najnowocześniejszej 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.

4. Pytania i odpowiedzi

Kiedy nie trzeba powiadamiać osób fizycznych?

- We wszystkich sytuacjach, w których naruszenie bezpieczeństwa nie stanowi naruszenia danych osobowych (zob. następne pytanie).
- We wszystkich sytuacjach, w których z oceny stopnia dotkliwości naruszenia wynika, że nie jest prawdopodobne, aby naruszenie danych osobowych wywarło niekorzystny wpływ na dane osobowe lub prywatność osoby, której dane dotyczą, zgodnie z wymogami właściwego organu.
- We wszystkich sytuacjach, w których dostawca wykazał zgodnie z wymogami właściwego organu, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie bezpieczeństwa. Przykładowo jeżeli naruszenie danych osobowych (dotyczące wyłącznie ich poufności) odnosi się do danych zaszyfrowanych z użyciem najnowocześniejszego algorytmu lub do danych zabezpieczonych z użyciem klucza haszującego/ciągu zaburzającego za pomocą najnowocześniejszej funkcji haszującej, a żadne zastosowane klucze tajne i ciągi zaburzające nie zostały złamane.
- Powiadomienie o naruszeniach danych opisanych w niniejszej opinii stanowi dobrą praktykę dla wszystkich administratorów danych, nawet jeżeli nie jest ono wymagane.

Kiedy naruszenie bezpieczeństwa stanowi naruszenie danych osobowych?

Naruszenie bezpieczeństwa stanowi naruszenie danych osobowych, jeżeli danymi, których dotyczy naruszenie, są dane osobowe zgodnie z definicją podaną w art. 2 lit. a) dyrektywy 95/46/WE: „»dane osobowe« oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość".

W opinii 4/2007 wyjaśnia się, że dotyczy to danych odnoszących się do danej osoby: „tożsamość osoby można ustalić bezpośrednio poprzez jej nazwisko lub pośrednio poprzez jej numer telefonu, numer rejestracyjny samochodu, numer ubezpieczenia społecznego, numer paszportu lub poprzez zestawienie istotnych kryteriów, które umożliwią odróżnienie tej osoby poprzez zawężenie grupy, do której ona należy (wiek, zajęcie, miejsce zamieszkania, itp.)". Dodatkowe wytyczne w tym zakresie są dostępne w opinii 4/2007.

Czy należy uwzględnić prawdopodobne skutki wtórne?

Tak, o naruszeniach danych należy powiadamiać osoby, których dane dotyczą, jeżeli takie naruszenie może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność takich osób. Należy zatem uwzględnić wszystkie potencjalne konsekwencje i niekorzystne skutki, na jakie mogą być narażone osoby, których dane dotyczą.

Przykład 1: *Doszło do ataku na strony internetowe firmy fonograficznej, w wyniku którego skradziono i opublikowano w internecie bazę danych użytkowników. Ujawnione dane osobowe obejmują imiona/nazwiska, preferencje muzyczne oraz nazwy użytkowników i hasła użytkowników zarejestrowanych na stronach internetowych firmy. Skutki objęły 9 000 użytkowników.*

Jeżeli chodzi o opisane naruszenie, może wydawać się, że bezpośredni niekorzystny wpływ na osoby fizyczne (tj. ujawnienie informacji dotyczących preferencji muzycznych) jest raczej ograniczony, w związku z czym mogą powstać wątpliwości co do konieczności powiadomienia osób, których dane dotyczą. Ponieważ jednak doszło do złamania haseł, administrator danych będzie musiał je odnowić. Proces ten będzie wymagał powiadomienia użytkowników o przyczynach odnowienia haseł. Ponadto prawdopodobne jest również, że wtórnym niekorzystnym skutkiem naruszenia jest naruszenie dotyczące poufności danych w odniesieniu do innego konta, ponieważ wielu użytkowników stosuje to samo hasło do różnych kont[12]. Osoba, której dane dotyczą, będzie w stanie ograniczyć tego rodzaju wtórne skutki, zmieniając hasła do wszystkich innych kont, które posiada. Dlatego też powiadomienie powinno również zawierać informacje dotyczące prawdopodobnych niekorzystnych skutków dotyczących innych kont, a zatem należy w nim zalecić stosowanie różnych haseł na poszczególnych stronach internetowych oraz odnowienie haseł do wszystkich kont, wobec których korzystano ze złamanego hasła.

Przykład 2: *Drugim przykładem mogą być dowody w sprawie karnej dotyczące jednej osoby fizycznej, zapisane na płycie CD wysłanej przesyłką poleconą do prawnika, która to płyta zostaje jednak zgubiona na poczcie.*

Bezpośrednie naruszenie dotyczy braku dostępu do danych. Wpływ naruszenia na osobę(-y), której(-ych) dane dotyczą, może być nieistotny lub bardzo poważny, w zależności od możliwości podjęcia na czas odpowiedniego działania.
Prawdopodobne jest jednak wystąpienie wtórnych niekorzystnych skutków, jeżeli płyta CD została wysłana bez odpowiedniego zabezpieczenia i uzyskano dostęp do zapisanych na niej danych. W praktyce osoba, która jest w posiadaniu płyty, może przeczytać dane, sprzedać je dziennikarzom itp. Tego rodzaju wtórne skutki mogą mieć bardzo poważny wpływ na daną(-e) osobę(-y) fizyczną(-e).

W tym przypadku, jeżeli płytę CD można ponownie przesłać na czas, bezpośredni wpływ na osobę fizyczną byłby nieistotny i nie wymagałby jej powiadomienia, natomiast potencjalne wtórne naruszenie może być bardzo poważne i zdecydowanie wymagałoby powiadomienia zainteresowanych osób fizycznych.

Czy zachodzi konieczność powiadomienia o naruszeniu, jeżeli dotyczy ono tylko jednej osoby?

Tak, w dyrektywie 2002/58/WE nie określa się minimalnej liczby osób, których musi dotyczyć naruszenie danych, aby konieczne było powiadomienie ich o takim naruszeniu. Artykuł 3 ust. 1 dyrektywy w sprawie łączności elektronicznej stanowi, że: „Jeśli istnieje

[12] Według ostatnich badań liczba użytkowników internetu, którzy stosują to samo hasło do różnych kont, waha się między 55 % – 80 %.

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".

Administrator danych powiadamia zatem o naruszeniu w zależności od prawdopodobnych niekorzystnych skutków naruszenia, bez względu jednak na liczbę osób, których dane dotyczą i na które naruszenie ma wpływ.

Jak postępować w przypadku danych, które mogą być publicznie dostępne?

Należy rozważyć dwie kwestie.

1. Określenie „publicznie dostępne" może oznaczać różne stopnie dostępności: dane mogą być swobodnie dostępne przez internet, publicznie dostępne w ramach danej usługi abonenckiej, publicznie dostępne *offline* na żądanie itp.
   Przykładowo we Francji rejestr wyborców jest wywieszany na ścianach ratusza podczas wyborów i każdy wyborca lub każda partia polityczna może mieć do niego dostęp, jednak prawo nie dopuszcza publikacji takich list w internecie.
   Przypadkowe wysłanie wersji elektronicznej rejestru do niewłaściwego wyborcy lub utrata wersji papierowej listy nie stanowiłyby naruszenia dotyczącego poufności danych, którym byłaby natomiast publikacja listy w internecie, o której należałoby powiadamiać.

2. Określone dane mogą być publicznie dostępne dla określonych osób, których dane dotyczą, natomiast niedostępne dla innych osób.
   Przykładowo wykaz numerów telefonów powiązanych z nazwiskiem może zawierać zarówno numery publicznie dostępne w książce telefonicznej, jak i numery zastrzeżone.

Podsumowując, we wszystkich sytuacjach, w których wskutek naruszenia zachodzi zmiana stopnia dostępności lub jawności danych, należy uznać, że takie naruszenie dotyczy poufności danych i należy o nim powiadomić (jeśli istnieje prawdopodobieństwo, że naruszenie wywoła niekorzystne skutki dla osób, których dane dotyczą).

W jaki sposób dokonać powiadomienia, jeżeli dane kontaktowe osób fizycznych, których dotyczy naruszenie, są niewystarczające lub nieznane?

Zdarzają się przypadki, w których nawet dostawca związany z użytkownikiem końcowym bezpośrednim stosunkiem umownym nie posiada danych wystarczających do zapewnienia właściwego powiadomienia. W tym znaczeniu, uwzględniając nawet możliwość powiadomienia za pomocą ogłoszeń w mediach, nadal ma zastosowanie obowiązek podjęcia wszelkich odpowiednich starań w celu przekazania indywidualnych powiadomień[13].

[13] Zgodnie z art. 3 ust. 7 rozporządzenia nr 611/2013, jeżeli mimo odpowiednich starań dostawca nie jest w stanie zidentyfikować wszystkich osób fizycznych, wobec których naruszenie danych osobowych prawdopodobnie ma niekorzystne skutki, w mającym zastosowanie terminie dostawca powiadomi te osoby poprzez ogłoszenia w głównych mediach krajowych lub regionalnych w danych państwach członkowskich. Jednocześnie stwierdza się, że dostawca nadal podejmuje odpowiednie starania, by zidentyfikować te osoby i jak najszybciej przekazać im informacje.

Chociaż podejmowanie odpowiednich starań należy do obowiązków dostawcy, który musi posiadać wszystkie odpowiednie mechanizmy w celu zapewnienia, aby wszystkie osoby, których dotyczy naruszenie, zostały o takim naruszeniu powiadomione, nie wyklucza to jednak możliwości zwrócenia się z prośbą o wsparcie do innych dostawców lub kontrolerów danych posiadających dane kontaktowe takich osób. Dlatego też, jeżeli chodzi o przykład 4, kontroler danych nieposiadający danych kontaktowych właścicieli kart, których dotyczyło naruszenie, mógłby zgłosić naruszenie podmiotowi pośredniczącemu przy dokonywaniu płatności, który może z łatwością skontaktować się z danymi osobami fizycznymi. Inne przypadki mogą wymagać współpracy z właściwymi organami, które w każdym przypadku należy powiadomić, że dostawca nie może zagwarantować dokonania indywidualnych powiadomień.

Czy konieczne jest powiadamianie osób, których dane dotyczą, a na które nie miało wpływu naruszenie?

Nie, pod warunkiem że w sposób wiarygodny można stwierdzić, na które osoby, których dane dotyczą, naruszenie nie miało wpływu. Przykładowo, jeżeli można wykazać, że zdarzenie naruszające ochronę nie miało wpływu na określoną podgrupę osób, których dane dotyczą, wówczas takich osób nie trzeba powiadamiać o naruszeniu. Podejmując taką decyzję, administrator danych musi jednak rozważyć wszystkie prawdopodobne niekorzystne skutki. W zależności od charakteru naruszenia, nieotrzymanie powiadomienia może również stanowić stres dla osób fizycznych.