www.pwc.com

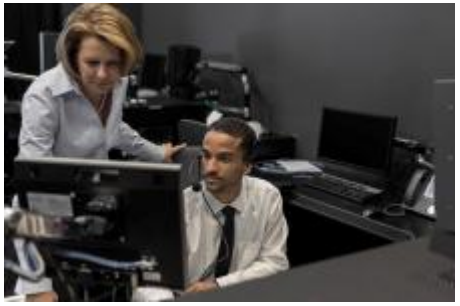
Opinia 3/2014 Grupy Roboczej art. 29 – zgłaszanie naruszeń danych osobowych

Anna Kobylańska
adwokat, PwC Legal
1 lipca 2014

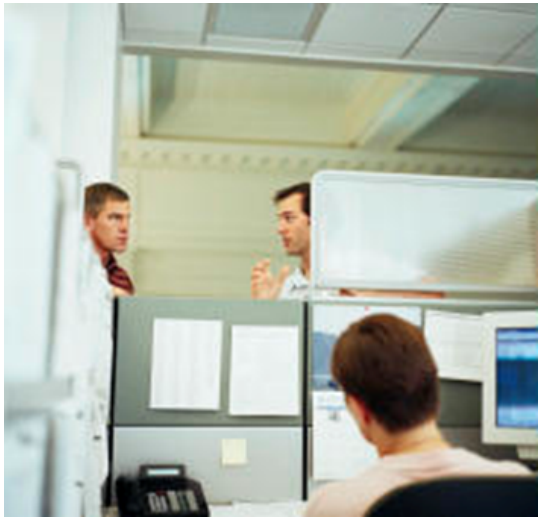
pwc

Opinia 3/2014 o powiadamianiu o naruszeniu danych osobowych

- przyjęta 25 marca 2014
- wskazówki dotyczące ustalania, kiedy należy powiadomić osoby, których dane osobowe dotyczą, o naruszeniu ich danych
- wskazówki co do kryteriów dokonywania takiej oceny
- wskazówki dotyczące środków zmniejszających ryzyko naruszenia danych osobowych



Naruszenie danych osobowych



Definicja z dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

„**Naruszenie danych osobowych**" oznacza 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

Obowiązek powiadomienia o naruszeniu

Dyrektywa 2002/58/WE	Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne
Gdy naruszenie danych osobowych może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność abonenta lub osoby fizycznej, dostawca publicznie dostępnych usług łączności elektronicznej bez zbędnej zwłoki powiadamia o takim naruszeniu abonenta lub osobę fizyczną	Gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca publicznie dostępnych usług telekomunikacyjnych niezwłocznie, nie później niż w terminie 3 dni od stwierdzenia naruszenia, zawiadamia o takim naruszeniu abonenta lub użytkownika końcowego

Obowiązek powiadomienia o naruszeniu

Przez naruszenie danych osobowych, które może wywrzeć niekorzystny wpływ na osobę, której dane dotyczą, rozumie się takie naruszenie, które może skutkować :

- nieuprawnionym posługiwaniem się danymi osobowymi,
- szkodą majątkową,
- naruszeniem dóbr osobistych,
- ujawnieniem tajemnicy bankowej lub innej ustawowo chronionej tajemnicy zawodowej.

Powiadomienie nie jest wymagane, jeżeli dostawca wykazał, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie (tego rodzaju środki muszą sprawiać, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich).

Szczegółowe wymagania dotyczące dokonywania powiadomień

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

- okoliczności, jakie należy uwzględnić przy ocenie konieczności dokonania powiadomienia
- obowiązek dokonania powiadomienia bez zbędnej zwłoki; możliwość opóźnienia powiadomienia
- obowiązek przekazania informacji w sposób jasny i łatwo zrozumiały; zakaz wykorzystywania powiadomienia do reklamy usług

Opinia 3/2014 - zastosowanie

- opinia zawiera wskazówki ułatwiające podjęcie decyzji, czy należy powiadomić osoby, których dane osobowe dotyczą, o naruszeniu ich danych

- opinia ma zastosowanie do:
  - obowiązku zawiadomienia wynikającego z przepisów prawa,
  - planowanych przepisów Rozporządzenia UE o ochronie danych osobowych,
  - dobrej praktyki zawiadamiania o naruszeniu w przypadkach, w których przepisy nie nakazują takiego dokonywać takiego powiadomienia

Opinia 3/2014

- wskazanie przypadków obowiązkowego zawiadamiania o naruszeniu (z przepisów dyrektywy UE)
- wskazanie wyjątków od tego obowiązku
- zawiadomienie osób, których dane dotyczą, nie powinno być uzależniane przez administratora danych od uprzedniego powiadomienia organu
- jeśli administrator danych ma wątpliwości, czy w danym przypadku powinien powiadomić osoby, których dane dotyczą, czy też może tego nie robić, powinien dokonać powiadomienia
- liczba osób, na które naruszenie ma wpływ, nie ma znaczenia (nawet przy niewielkiej liczbie osób, trzeba dokonać powiadomienia)

Opinia 3/2014

- lista przypadków, gdy powinno się dokonywać powiadomienia
  - skradziony laptop
  - włamanie na stronę internetową
  - udostępnienie loginu i hasła przez pracownika
  - wyrzucenie koperty z danymi do kosza

- kryteria oceny skutków dla osób, których dane osobowe dotyczą
- wskazanie środków, które mogą ograniczać ryzyko naruszeń
- przypadki, w których nie trzeba dokonywać powiadomienia
  - udostępnienie zaszyfrowanych danych bez ujawienia klucza
  - zastosowanie kodowania mieszającego bez ujawnienia klucza

Dziękuję

Anna Kobylańska

anna.kobylanska@pl.pwc.com

tel. +48 22 746 6226