Vol.30

WYTYCZNE UODO DOTYCZĄCE ZGŁASZANIA NARUSZEŃ

Compliance Insights

KONIECZNY WIERZBICKI

KANCELARIA RADCÓW PRAWNYCH

1 NAJNOWSZE WYTYCZNE UODO

23 stycznia w trakcie współorganizowanej przez Urząd Ochrony Danych Osobowych konferencji „Ocena ryzyka a ochrona danych osobowych” **przedstawiciele UODO zaprezentowali rygorystyczne stanowisko dotyczące zgłaszania naruszeń ochrony danych osobowych do Prezesa UODO** (PUODO).

2 TRZY KLUCZOWE ASPEKTY

Podczas konferencji poruszono trzy ważne z punktu widzenia praktyki aspekty:

- kiedy należy zgłaszać naruszenie do PUODO,
- czy to, że naruszenie wystąpiło, oznacza, że administrator zawinił i ponosi za nie odpowiedzialność,
- kiedy można powołać się na dostęp do danych przez zaufanego odbiorcę.

3 CZY TRZEBA ZGŁASZAĆ INCYDENT DO PUODO?

Zgodnie z art. 33 ust. 1 RODO, **w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu (w Polsce – PUODO)**, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Przedstawiciele UODO wskazali, że ten obowiązek należy interpretować rygorystycznie i tylko w wyjątkowych przypadkach administrator może powołać się na przesłanki wyłączające obowiązek zgłoszenia naruszenia.

4 KIEDY TRZEBA ZGŁASZAĆ NARUSZENIE DO PUODO?

Najnowsze wytyczne opierają się na trzystopniowym modelu postępowania:

- **Brak ryzyka** – naruszenie należy wyłącznie 1) udokumentować,
- **Wystąpienie ryzyka** – jeżeli naruszenie może generować ryzyko (i to jakiekolwiek), należy je 1) udokumentować i 2) zgłosić do Prezesa UODO,
- **Wysokie ryzyko** – jeżeli naruszenie może generować wysokie ryzyko, należy je 1) udokumentować, 2) zgłosić do Prezesa UODO i 3) zawiadomić o tym naruszeniu osoby, których dane te dotyczą.

5 CO SIĘ ZMIENIA?

Dotychczas w praktyce często stosowane było podejście, zgodnie z którym – niskie ryzyko naruszenia = brak potrzeby zgłoszenia naruszenia do PUODO.

Przedstawiciele PUODO zaprezentowali odmienne stanowisko i wprost podkreślili, że tylko brak jakiegokolwiek ryzyka wyłącza obowiązek zgłoszenia naruszenia.

Jeśli ryzyko jest niskie, ale istnieje – naruszenie należy zgłosić do PUODO.

6 CZY ADMINISTRATOR PONOSI WINĘ ZA NARUSZENIE?

Jak podkreślono na konferencji, samo zgłoszenie naruszenia do organu nadzorczego nie oznacza automatycznie, że administrator ponosi winę za wystąpienie tego zdarzenia.

Zgłoszenie naruszenia to jedynie zawiadomienie organu o pewnym fakcie. Dopiero w toku czynności wyjaśniających może się okazać, że administrator rzeczywiście zawinił, i jeśli tak – może ponieść negatywne konsekwencje na gruncie RODO.

Samo jednak naruszenie ochrony danych osobowych nie oznacza automatycznie naruszenia przepisów RODO – to, że doszło do naruszenia nie oznacza, że postąpiono niezgodnie z przepisami.

7 KIEDY MOŻNA MÓWIĆ O ZAUFANYM ODBIORCY?

Pojęcie „zaufanego odbiorcy" pozwala obniżyć ryzyko związane z naruszeniem ochrony danych osobowych i nie zgłaszać naruszenia do PUODO, jeśli dane przypadkowo zostały ujawnione takiemu zaufanemu odbiorcy.

Organ zastosował restrykcyjne podejście do zdefiniowania tego podmiotu. O „zaufanym odbiorcy" można mówić wtedy, gdy znane są administratorowi szczegóły dotyczące funkcjonowania tego podmiotu np. znajomość wewnętrznie obowiązujących procedur w zakresie ochrony danych osobowych.

Dodatkowo wskazano, że nie można automatycznie uznać żadnego podmiotu za „zaufanego odbiorcę", w tym nawet podmiotu publicznego. Każdy przypadek wymaga indywidualnej analizy.

8 PORADNIK UODO

Na konferencji zapowiedziano, że nowe wytyczne pojawią się w zaktualizowanym wydaniu poradnika UODO dotyczącego oceny ryzyka w przypadku naruszenia ochrony danych osobowych.

Publikacja poradnika spodziewana jest na dniach – warto śledzić najnowsze aktualności i informacje, aby się z nim zapoznać.

9 JAK NOWE WYTYCZNE WPŁYWAJĄ NA ADMINISTRATORÓW DANYCH?

Nowe wytyczne Urzędu Ochrony Danych Osobowych będą najprawdopodobniej stosowane przez urząd jeszcze przed publikacją zaktualizowanego poradnika. Co to oznacza?

- Warto przejrzeć obowiązujące w firmie procedury dotyczące naruszeń ochrony danych osobowych, aby mieć pewność, że są one zgodne z najnowszymi wytycznymi.
- W przypadku wystąpienia naruszenia – nawet, jeśli zastosowana metodyka oceny ryzyka (np. ENISA) wskazuje na nisko ryzyko, naruszenie lepiej zgłosić, niż nie zgłaszać go wcale.
- Na ujawnienie danych „zaufanemu odbiorcy" można powołać się jedynie, jeśli jest to dla nas podmiot znany i wiemy, jakie procedury dotyczące ochrony danych osobowych u niego funkcjonują.

Kontakt

PARTNER
MARIUSZ PURGAŁ
mariusz.purgal@kwkr.pl

ASSOCIATE
ALICJA ŁOPACIŃSKA
alicja.lopacinska@kwkr.pl

ZESPÓŁ COMPLIANCE KWKR

PAWEŁ ZYSKOWSKI

KATARZYNA KANIK

ANNA BARTOSIAK

BARTOSZ BOGUSŁAWSKI

JUSTYNA STASZKIEWICZ

AGATA BACA