

COMPLIANCE INSIGHTS

Vol. 64

Zawiadamianie
osób przy
naruszeniu
danych – wnioski
z wyroku NSA



1. Zasady RODO

Nie każde naruszenie ochrony danych oznacza automatycznie konieczność zawiadomiania podmiotów danych.

Kluczowe znaczenie ma ocena ryzyka dla ich praw i wolności.

Ta ocena jest elementem oceny zdarzenia i możliwych konsekwencji naruszenia. Jeśli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi nie tylko zgłosić naruszenie do PUODO, ale także zawiadomić osoby, których dane dotyczą.



2. Przedmiot sprawy

W analizowanej sprawie doszło do wysyłki wiadomości e-mail z niezaszyfrowanym załącznikiem zawierającym dane osobowe – imię, nazwisko, numer PESEL oraz informacje finansowe – do niewłaściwego odbiorcy.

Administrator nie zgłosił naruszenia do organu nadzorczego ani nie powiadomił o incydencie osoby, której dane ujawniono, uznając, że ryzyko wiążące się z naruszeniem jest znikome. Sprawa trafiła do PUODO, a następnie do sądu administracyjnego.



3. Stanowisko PUODO

PUODO uznał, że ujawnienie takiego zestawu danych, nawet gdy dotyczy tylko jednej osoby, stanowi poważne naruszenie ochrony danych.

W ocenie organu, nie dowody na wykorzystanie tych danych, a sam fakt ich ujawnienia tworzy wysokie ryzyko dla praw lub wolności osoby fizycznej.

Kluczowe znaczenie ma ryzyko związane z wagą i skutkiem naruszenia, a nie prawdopodobieństwo, czy to ryzyko się ziści. Dlatego obowiązek zawiadomienia był w pełni uzasadniony.



4. Wyrok WSA

WSA nie zgodził się z decyzją PUODO i przyznał rację administratorowi.

Zdaniem Sądu, ujawnienie danych jednej osoby nie rodziło istotnego ryzyka, zwłaszcza że odbiorca pliku był znany i nie wykorzystał informacji w sposób niezgodny z prawem.

W ocenie WSA, organ nie wykazał, że taka sytuacja mogła powodować istotne negatywne konsekwencje dla osoby, której dane zostały ujawnione. Sąd uchylił decyzję organu, co doprowadziło do wniesienia skargi kasacyjnej.



5. Ocena NSA

Naczelny Sąd Administracyjny przychylił się do stanowiska PUODO i wskazał, że samo potencjalne ryzyko dla praw i wolności osoby fizycznej wystarczy do uznania naruszenia za poważne. Sprawa trafi więc ponownie do rozpatrzenia przez WSA.

Dane takie jak imię, nazwisko i PESEL mogą być wykorzystane do kradzieży tożsamości, zaciągania zobowiązań lub uzyskiwania dostępu do świadczeń medycznych. Dlatego administrator powinien nie tylko zgłosić naruszenie, ale i powiadomić osobę, której dane ujawniono.



6. Kryteria oceny ryzyka

NSA przypomniał, że administrator musi oceniać ryzyko naruszenia nie w oparciu o subiektywne przekonania, ale przy użyciu obiektywnych kryteriów, tj. np. dotychczasowe doświadczenia dotyczące podobnych spraw czy wiedza z zakresu bezpieczeństwa informacji.

Znaczenie mają także okoliczności samego naruszenia, np. rodzaj i kategorie danych, liczba osób dotkniętych naruszeniem, okoliczności naruszenia i możliwość wykorzystania danych przez osoby trzecie.



6. Kryteria oceny ryzyka

Aby administrator nie musiał zgłaszać naruszenia do PUODO, musi istnieć niskie prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych – nie samego naruszenia tych praw w wyniku naruszenia.

Wystarczy, że istnieje potencjał naruszenia praw osoby fizycznej – nie trzeba czekać, aż negatywne skutki faktycznie wystąpią.

Wysokie ryzyko dla praw lub wolności osoby fizycznej wystarczy, by uruchomić obowiązek zawiadomienia.



7. Znaczenie numeru PESEL

Sąd jednoznacznie wskazał, że ujawnienie numeru PESEL stanowi realne zagrożenie.

Ten identyfikator jest szeroko wykorzystywany w kontaktach z instytucjami finansowymi, publicznymi i prywatnymi. W połączeniu z innymi danymi umożliwia podszycie się pod daną osobę czy wyłudzenie kredytu lub pożyczki na jej dane.

Dlatego samo jego ujawnienie może tworzyć wysokie ryzyko dla praw i wolności osoby fizycznej.



8. Wnioski praktyczne

Każde naruszenie należy analizować indywidualnie, z uwzględnieniem rodzaju danych i skutków ich ujawnienia.

Administrator powinien dokumentować proces oceny ryzyka oraz motywy stojące za decyzją o zgłoszeniu naruszenia lub jego braku.

Nie wystarczy założyć, że incydent jest błahy – brak zgłoszenia bez uzasadnienia może być uznany przez PUODO za naruszenie obowiązków wynikających z art. 33 i 34 RODO i skutkować nałożeniem kary pieniężnej.



9. Podsumowanie

Wyrok NSA przypomina, że obowiązek zawiadamiania osób fizycznych o naruszeniu ich danych nie jest automatyczny, ale **wymaga starannej i udokumentowanej oceny ryzyka.**

Kluczem jest podejście proporcjonalne, oparte na realnych skutkach ujawnienia danych. W dobie rosnącej liczby incydentów warto traktować każdy przypadek poważnie i wdrażać procedury reagowania, które chronią nie tylko dane, ale też zaufanie klientów.



Kontakt



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl



Alicja Łopacińska

Associate

alicja.lopacinska@kwkr.pl

Zespół Compliance KWKR



**Agata
Baca**



**Katarzyna
Kanik**



**Anna
Bartosiak**



**Paweł
Zyskowski**



**Aneta
Kiser**



**Justyna
Staszkiwicz-Maj**