Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji — **16 listopad 2022 r.**

Podmiot kontrolowany — **P4 Sp. z o.o.**

Wysokość kary — **1 599 395 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b) i lit. d), art. 32 ust. 2 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W styczniu 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła skarga od Virgin Mobile Polska Sp. z o.o. (obecnie P4 Sp. z o.o., dalej: Spółka), której przedmiotem było zaskarżenie w całości decyzji Prezesa UODO o numerze DKN.5112.1.2020 oraz zawnioskowanie o jej uchylenie.

Opis wydarzeń:

1) Spółka w piśmie przedstawiła następujące zarzuty wskazując, iż w decyzji przyjęto:

a) błędny czas trwania naruszenia,

b) założenie, że osoby, których dotyczyło naruszenie, poniosły szkodę,

c) zwiększenie administracyjnej kary pieniężnej za nieumyślne naruszenie RODO podczas, gdy w takiej sytuacji kara powinna być zmniejszona,

d) brak przyjęcia jako czynniki łagodzące karę następujących elementów: brak wcześniejszego naruszenia, kategoria danych osobowych, brak osiągnięcia przez Spółkę korzyści finansowych, uniknięcie przez Spółkę straty,

e) jako czynnik obciążający okoliczności przetwarzania danych osobowych w sposób profesjonalny uznając to za znaczący wpływ na dużą wagę naruszenia,

f) niewdrożenie środka bezpieczeństwa organizacyjnego polegającego na regularnym testowaniu, mierzeniu i ocenianiu skuteczności środków technicznych i organizacyjnych jako bezpośredniej przyczyny niewykrycia podatności będącej przyczyną naruszenia ochrony danych,

g) wyższą karę za naruszenie tego samego czynu naruszając tym samym zasadę proporcjonalności wymiaru kary,

h) założenie, że do naruszenia może dojść pomimo braku wyrządzenia szkody,

i) błędną liczbę osób dotkniętych naruszeniem,

j) błędny zakres danych osobowych osób dotkniętych naruszeniem,

k) błędny czas trwania naruszenia obowiązku regularnego testowania, mierzenia i oceniania środków zabezpieczenia,

l) błędne założenie, że uprawnienia, którymi dysponował atakujący pozostają bez znaczenia dla stwierdzenia naruszenia,

m) fakty i dowody, które utrudniają rekonstrukcję sposobu rozumowania UODO.

2) 21 października 2021 r. Wojewódzki Sąd Administracyjny w Warszawie uchylił zaskarżoną decyzję.

3) Wojewódzki Sąd Administracyjny w Warszawie uznał, iż Prezes UODO nie wyjaśnił w uzasadnieniu decyzji, dlaczego przy zastosowaniu kary na jej wysokość nie miały wpływu czynniki takie jak:

a) działania podjęte w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,

b) brak wcześniejszych naruszeń,

c) sposób dowiedzenia się o naruszeniu,

d) pobranie jedynie ok. 13,62% wszystkich rekordów znajdujących się w bazie danych,

e) liczba realnie poszkodowanych osób,

f) zakres naruszonych danych osobowych,

g) kategoria danych osobowych,

h) brak osiągnięcia korzyści finansowych w związku z naruszeniem,

i) podejmowanie przez Spółkę działań zmierzających do wyeliminowania nieprawidłowości.

4) Wojewódzki Sąd Administracyjny w Warszawie podtrzymał decyzje UODO w zakresie oceny, że Spółka:

a) przetwarzała dane osobowe klientów w sposób niezapewniający odpowiedni stopień bezpieczeństwa danych osobowych,

b) nie wdrożyła procedur dotyczących regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,

c) poprzez brak powyższego działania doprowadziła do wystąpienia naruszenia ochrony danych osobowych,

d) nie przeprowadziła weryfikacji zabezpieczeń aplikacji pod kątem podatności systemu informatycznego,

e) wdrożyła system bez poprawnie działającej walidacji.

5) W związku z powyższym, Prezes UODO dokonał ponownej analizy materiału dowodowego zgromadzonego w toku postępowania.

6) Prezes UODO podtrzymał swoją opinię jakoby brak w przyjętych przez Spółkę procedurach uregulowań zapewniających regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych przyczynił się do wystąpienia naruszenia danych osobowych.

Przyczyna naruszenia:

Spółka nie przeprowadzała regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Decyzja PUODO:

Kara pieniężna w wysokości 1.599.395 PLN.

Źródło:

https://uodo.gov.pl/decyzje/DKN.5112.1.2020

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Wykonywanie regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

2) Uwzględnienie w Polityce Ochrony Danych Osobowych kwestii dotyczących regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3) Weryfikacji doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz ocena weryfikacji przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

4) Przeprowadzanie testów nastawionych na weryfikację zabezpieczeń programów i aplikacji.

5) Wykonanie udokumentowanej analizy ryzyka uwzględniającej charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

6) Oparcie przeglądu, sprawdzenia lub audytu na kompletnych i rzetelnych informacjach.

7) Realizacja zasady rozliczalności w kontekście zachowania staranności zarówno przy nadawaniu upoważnień do przetwarzania danych, jak i również przy cofaniu upoważnień względem byłego pracownika, zleceniobiorcy czy wykonawcy.

8) Odebranie uprawnień w systemie informatycznym osobom, którym wygasło upoważnienie.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska