Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Data wydania decyzji

14.12.2020 r.

Podmiot kontrolowany

Virgin Mobile Polska Sp. z o.o.

Wysokość kary

1 968 524,00 PLN

Rodzaj naruszenia

Naruszenie Art. 5 (1) f) RODO, Art. 5 (2) RODO, Art. 25 (1) RODO, Art. 32 (1) b) RODO, Art. 32 (1) d) RODO, Art. 32 (2) RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

W grudniu 2019 roku Virgin Mobile Polska Sp. z o.o. zgłosiła do Prezesa UODO naruszenie polegające na uzyskaniu przez osobę nieuprawnioną dostępu do danych osobowych abonentów usług przedpłaconych i pozyskaniu 142 222 rekordów potwierdzeń ich rejestracji. Naruszenie pełnego zakresu danych osobowych wystąpiło wyłącznie w 4522 przypadkach. Odnosiło się do imion i nazwisk, numerów PESEL i numerów dokumentów abonentów. W pozostałym zakresie, naruszenie odnosiło się do: imion, nazwisk oraz numerów PESEL (108702 przypadków) lub numerów dokumentu abonenta (10167 przypadków).

W związku ze zgłoszonym naruszeniem pracownicy UODO dokonali w Spółce kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Zakresem kontroli objęty został sposób przetwarzania danych, w tym sposób zabezpieczenia danych, w ramach świadczenia usług telekomunikacyjnych abonentom usług przedpłaconych. Na podstawie informacji i dowodów zgromadzonych w toku kontroli pracownicy UODO ustalili, iż Spółka naruszyła zasadę poufności danych poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych służących do rejestracji danych osobowych abonentów usług przedpłaconych, co doprowadziło do uzyskania przez osobę nieuprawnioną dostępu do tych danych.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1. Regularnie testuj, mierz i oceniaj skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

2. Uwzględnij w Polityce Ochrony Danych Osobowych kwestie dotyczące regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

3. Weryfikuj dobór i poziom skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceniaj je przez pryzmat adekwatności do ryzyk i proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

4. Przeprowadzaj testy nastawione na weryfikację zabezpieczeń programów i aplikacji.

5. Wykonaj i udokumentuj analizę ryzyka uwzględniającą charakter zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

6. Przeglądy, sprawdzenia lub audyty opieraj na kompletnych i rzetelnych informacjach.

7. Realizuj zasadę rozliczalności w kontekście zachowania staranności zarówno przy nadawaniu upoważnień do przetwarzania danych, jak również przy ich cofaniu wobec byłego pracownika, zleceniobiorcy, czy wykonawcy.

8. Odbieraj uprawnienia w systemie informatycznym osobom, którym wygasło upoważnienie.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak