Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **22 kwietnia 2021 r.**

Podmiot kontrolowany **Cyfrowy Polsat S.A.**

Wysokość kary **1 136 975 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 32 ust. 1 i 2 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Cyfrowy Polsat S.A. (Spółka) regularnie dokonywał zgłoszeń do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszeń ochrony danych osobowych swoich klientów, które polegały m.in. na utracie przez kurierów dokumentów zawierających dane osobowe klientów lub na wydaniu przez kurierów niewłaściwej osobie dokumentów zawierających dane osobowe w postaci: imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, adresu e-mail, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz danych dotyczących łączących strony umów.

Opis wydarzeń:

1) Prezes UODO po przeanalizowaniu zgłoszeń zwrócił się do Spółki o złożenie wyjaśnień w przedmiotowej sprawie.
2) Spółka w odpowiedzi na pismo wyjaśniła, iż:
a) została zapewniona przez przewoźnika o bieżącym monitorowaniu skali naruszeń, jak i podejmowaniu działań mających na celu wyeliminowanie lub zminimalizowanie tego typu przypadków naruszeń,
b) wyjaśnia na bieżąco z przewoźnikiem przypadki naruszeń, celem wyeliminowania problemu opóźnień w przekazywaniu informacji o utracie danych.
3) W swych wyjaśnieniach Spółka dodatkowo wyodrębniła trzy typy naruszeń:
a) zdarzenia dotyczące wydania przesyłki osobie trzeciej, gdzie w większości przypadków osobą trzecią jest członek najbliższej rodziny zamieszkały pod wspólnym adresem z klientem;
b) zagubienie dokumentów przez firmę kurierską;
c) kradzież przesyłki ze sprzętem.
4) Spółka wskazała, że dokonała szczegółowej oceny ryzyka naruszeń dla każdej z trzech wyżej wymienionych kategorii zdarzeń i na podstawie metodologii ENISA określiła poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą, jako niski
5) Spółka poinformowała również, że pomimo analizy naruszeń, której wynik pozwolił określić poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą, jako „niski", zgłaszała jednak te naruszenia ze względu na wytyczne Prezesa UODO, wskazujące na konieczność notyfikowania zdarzeń, które obejmowały nr PESEL, uwzględniając ryzyko jako „wysokie".
6) W odpowiedzi na powyższe Prezes UODO uznał, iż:
a) Spółka w formularzach zgłoszenia wskazywała na wysokie ryzyko naruszenia praw lub wolności osób fizycznych w związku z tymi naruszeniami pomimo dokonywanej przez siebie odmiennej oceny tego ryzyka oraz nie podważała wówczas dokonanej przez Prezesa UODO oceny,
b) Spółka nie dokonywała analizy relacji łączących odbiorcę przesyłki z klientem, a tym samym nie oceniała czy osoba odbierająca przesyłkę była zaufanym odbiorcą,
c) naruszenie poufności danych, w szczególności danych dotyczących łącznie imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz innych kategorii danych dotyczące łączących strony umów (np. ID kontraktu, numer umowy, numer dokumentu, numer sprzętowy, numer i kwota faktury VAT, numer konta do wpłat), powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w związku z czym konieczne jest zawiadomienie osoby, której dane dotyczą, o naruszeniu jej danych osobowych,
d) Spółka nie wypracowała odpowiednich mechanizmów mających na celu kontrolę realizacji przez podmiot przetwarzający swoich zobowiązań,
e) brak szybkiej reakcji ze strony przewoźnika nie zdejmuje ze Spółki odpowiedzialności za stwierdzenie naruszenia ochrony danych osobowych,
f) Spółka powinna wdrożyć odpowiednie rozwiązania umożliwiające weryfikację zobowiązań przewoźnika np. poprzez bieżące monitorowanie etapu doręczania przesyłek,
g) zapisy wdrożonych polityk i procedur są martwe i nie miały odzwierciedlenia w rzeczywistości, gdyż Spółka nie wdrożyła dostatecznych mechanizmów pozwalających na bieżące monitorowanie przesyłek kurierskich,
h) Spółka nie prowadziła dostatecznego nadzoru naruszeń, co w konsekwencji prowadziło do zawiadamiania osób, których dane dotyczyły, o naruszeniu ich danych osobowych po upływie nawet dwóch czy trzech miesięcy od daty naruszenia.

Przyczyna naruszenia:

Spółka w niewystarczający sposób dokonywała oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych znajdujących się na dokumentach dostarczanych klientom Spółki za pośrednictwem podmiotu świadczącego usługi kurierskie.

Decyzja PUODO:

Kara pieniężna w wysokości 1 136 975 PLN

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2) Dokonaj wdrożenia takich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzania danych osobowych i szybką identyfikację naruszeń ochrony danych osobowych.
3) Dokonuj weryfikacji doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceny weryfikacji przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.
4) Kontroluj podmioty przetwarzające m.in. w zakresie notyfikacji naruszeń ochrony danych osobowych.
5) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny, weź pod uwagę czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
6) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować ryzyko dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.
7) Jeśli masz wątpliwości co do oceny ryzyka dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia bezpieczeństwa danych osobowych, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.
8) Zapewnij ochronę danych osobowych na płaszczyźnie nie tylko formalnej (dokumentacja), ale i praktycznej.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak