Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **17 stycznia 2024 r.**

Podmiot kontrolowany **Morele.net Sp. z o. o.**

Wysokość kary **3 819 960 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

W listopadzie i grudniu 2018 roku Morele.net Sp. z o.o. (Morele) trzykrotnie zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszenie ochrony danych osobowych dotyczące uzyskania nieuprawnionego dostępu do bazy danych klientów sklepów internetowych oraz uzyskania nieuprawnionego dostępu do konta pracownika.

Opis wydarzeń:

1. W styczniu 2019 r. odbyła się kontrola UODO w Morele, której zakres obejmował przetwarzanie danych osobowych klientów sklepów internetowych.

2. Na podstawie zgromadzonego materiału dowodowego ustalono, że Morele naruszyło przepisy o ochronie danych osobowych i nałożono karę w wysokości 2 830 410 PLN.

3. W październiku 2019 r. Morele złożyło skargę do Wojewódzkiego Sądu Administracyjnego w Warszawie na decyzję Prezesa UODO.

4. We wrześniu 2020 r. Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę Morele uznając, że nie zasługuje ona na uwzględnienie.

5. W związku z powyższym Morele złożyło skargę kasacyjną od wyroku zaskarżając go w całości.

6. W lutym 2023 r. Naczelny Sąd Administracyjny uchylił zaskarżony wyrok i zaskarżoną decyzję uznając, że wniosek o przeprowadzenie dowodu z opinii biegłego był zasadny oraz poddając w wątpliwość czy pracownicy UODO posiadali specjalistyczną wiedzę, pozwalającą na ocenę odpowiedniości środków technicznych i organizacyjnych w działalności gospodarczej o tak dużej skali.

7. W związku z wykonaniem powyższego wyroku Naczelnego Sądu Administracyjnego, Prezes UODO wytworzył wewnętrzny dokument stanowiący wnioski z analizy standardu środków bezpieczeństwa stosowanych przez Morele oraz wydał postanowienie o odmowie uwzględnienia wniosku o dopuszczenie opinii biegłego.

8. W grudniu 2023 r. Morele wniosło o wyłączenie pracowników UODO od udziału w postępowaniu w sprawie ze względu na obawę co do bezstronności autorów analizy.

9. Prezes UODO nie przychylił się do tego wniosku i po zapoznaniu się z całością materiału dowodowego uznał, że Morele wykonywało analizę ryzyka doraźnie dla poszczególnych procesów oraz w sposób niesformalizowany, co skutkuje brakiem możliwości oceny adekwatności zastosowanych środków technicznych i organizacyjnych.

Przyczyna naruszenia:

Morele nie wdrożyło odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą.

Decyzja PUODO:

Kara pieniężna w wysokości 3 819 960 PLN.

Źródło:

https://uodo.gov.pl/decyzje/ZSPR.421.2.2019%20ZSPR.405.67.2019

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1. Dokonaj wdrożenia mechanizmu dwuetapowego uwierzytelniania do aplikacji i programów dostępnych z poziomu Internetu, w których przetwarzane są dane osobowe.

2. Dokonaj wdrożenia procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego.

3. Dokonaj wdrożenia procedur i systemu powiadamiania o nietypowych aktywnościach pracowników w panelu administracyjnym.

4. Dokonaj wdrożenia szyfrowania danych zapisanych w bazie danych.

5. Przechowuj techniczne hasła dostępowe w zaszyfrowanej bazie danych.

6. Dokonaj wdrożenia ograniczenia w zakresie IP, z którego można logować się do panelu administracyjnego.

7. Wykonuj regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

8. Wykonuj zewnętrzne audyty bezpieczeństwa.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska