

Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych



Data wydania decyzji

6 lipca 2022 r.



Podmiot kontrolowany

Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego



Wysokość kary

10 000 PLN

FORSAFE
BEZPIECZENSTWO PONAD WSZYSTKO


Rodzaj naruszenia

art. 33 ust. 1, art. 34 ust. 1 RODO

Niewystarczające wypełnienie obowiązku powiadomienia o naruszeniu danych.



Przedmiot decyzji

Źródło postępowania:

Do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja od Rzecznika Praw Pacjenta. Jej przedmiotem było poinformowanie o możliwości zaistnienia naruszenia ochrony danych osobowych w Uniwersyteckim Centrum Klinicznym Warszawskiego Uniwersytetu Medycznego z siedzibą w Warszawie (Uniwersyteckie Centrum Kliniczne).

Opis wydarzeń:

1) Rzecznik Praw Pacjenta w wysłanym piśmie poinformował, iż pacjent Uniwersyteckiego Centrum Klinicznego otrzymał od jednego z lekarzy skierowanie do poradni specjalistycznej zawierające dane osobowe dotyczące innej osoby w zakresie: imię, nazwisko, adres zamieszkania, numer PESEL oraz informacje o stanie zdrowia (informacja o rozpoznaniu i celu porady).

2) Prezes UODO zwrócił się do Uniwersyteckiego Centrum Klinicznego o ustosunkowanie się do treści pisma oraz złożenie wyjaśnień w przedmiotowej sprawie.

3) W reakcji na powyższe pismo Uniwersyteckie Centrum Kliniczne wskazało, iż nie dokonano zgłoszenia naruszenia ochrony danych osobowych ze względu na brak znaczących skutków dla naruszenia praw lub wolności osoby, której dane dotyczą.

4) Biorąc pod uwagę zaistniałą sytuację, Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Uniwersyteckie Centrum Kliniczne administracyjnej kary pieniężnej w związku z brakiem zgłoszenia naruszenia ochrony danych osobowych oraz brakiem zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dotyczyło naruszenie.

Przyczyna naruszenia:

Uniwersyteckie Centrum Kliniczne nie dokonało zgłoszenia naruszenia ochrony danych osobowych oraz nie zawiadomiło o naruszeniu ochrony danych osobowych osoby, której dane dotyczą.

Decyzja PUODO:

1) Kara pieniężna w wysokości 10 000 PLN

2) Nakaz zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych – w terminie 3 dni od dnia, w którym decyzja stanie się ostateczna.

Źródło:

<https://www.uodo.gov.pl/decyzje/DKN.5131.34.2021>



Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę:

a) konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia,

b) 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 sfalszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne,

c) liczbę osób fizycznych, na które naruszenie wywiera wpływ

2) Ocenę ryzyka naruszenia praw lub wolności osoby fizycznej dokonaj przez pryzmat osoby dotkniętej naruszeniem, a nie interesów Administratora.

3) 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.

4) 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.

5) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, dokonaj zawiadomienia osób fizycznych, których dane dotyczą, o zaistniałym naruszeniu. Zawiadomienia należy wykonać bez zbędnej zwłoki.

6) Pamiętaj, że obowiązek zawiadomienia osoby fizycznej o naruszeniu nie jest uzależniony od materializacji negatywnych konsekwencji dla takiej osoby, ale od samej możliwości wystąpienia takiego ryzyka.

7) Nie wykonuj oceny naruszenia ochrony danych osobowych w sposób schematyczny, gdyż każda ocena jest inna i należy do niej podchodzić indywidualnie.

