Naruszenie przepisów RODO

_case study 1.0

Analiza

Sygnatura: DKN.5131.34.2021

Data: dnia 06 lipca 2022 r.

Administrator: Uniwersyteckie Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego

Wysokość kary: 10 000 zł

Rodzaj naruszenia:

- art. 33 ust. 1 RODO

  niezgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia;

- art. 34 ust. 1 RODO

  niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą.

Opis naruszenia:

Pacjent otrzymał od jednego z lekarzy będącego pracownikiem Uniwersyteckiego Centrum Klinicznego Warszawskiego Uniwersytetu Medycznego (dalej: „**Administrator**") skierowanie do poradni specjalistycznej zawierające dane osobowe dotyczące innej osoby w zakresie:

1. imię i nazwisko;
2. adres zamieszkania;
3. numer ewidencyjny PESEL;
4. informacje o stanie zdrowia, tj. informacja o rozpoznaniu i celu porady.

Źródło postępowania:

Do UODO wpłynęła informacja o możliwości zaistnienia naruszenia ochrony danych osobowych od Rzecznika Praw Pacjenta.

Okoliczności sprawy:

1. Po powzięciu informacji o możliwym naruszeniu ochrony danych osobowych Prezes UODO zwrócił się do Administratora o przekazanie informacji, czy w związku z możliwością wystąpienia naruszenia ochrony danych osobowych została dokonana analiza incydentu pod kątem ryzyka naruszenia praw lub wolności osób fizycznych
2. W odpowiedzi na wyżej wskazane wezwanie Administrator udzielił wyjaśnień, iż:
   (a) Administrator dokonał wstępnej uproszczonej analizy poziomu ryzyka zdarzenia;
   (b) Administrator zakwalifikował zdarzenie jako incydent bezpieczeństwa oraz podjął decyzje o niedokonaniu zgłoszenia Prezesowi UODO, jak również osobom, których dane dotyczą, ze względu na fakt, iż *„potencjalnie pokrzywdzona została jedna osoba fizyczna, której to dane ujawnione zostały jednej, możliwej do zidentyfikowania osobie w wąskim i błędnym zakresie*";
   (c) Administrator przedłożył także „Formularz oceny skutków naruszenia ochrony danych osobowych";
   (d) Zgodnie z wyjaśnieniami lekarza, pacjent P.Ż skierowany został do poradni, jednak po pewnym czasie wrócił, twierdząc, iż nie może zapisać się na wskazane badania. W związku z powyższym lekarz ze względu na pośpiech użył nie tej karty choroby i omyłkowo wpisał inne dane pacjenta. Dane wpisane zostały na pacjenta A.W., jednak pacjent z takimi danymi nie istnieje, a dane należały do pacjentki A.W.
3. Prezes UODO wszczął z urzędu postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych.

Wnioski Prezesa UODO:

1. Zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO pozwalają organowi nadzorczemu na właściwą reakcję mogącą ograniczyć skutki naruszeń;
2. Informacje, że osoba jest pacjentem przychodni stanowi samo w sobie informacje o stanie zdrowia oraz zwiększa możliwość identyfikacji osoby;
3. Stosownie do art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności, numer PESEL jednoznacznie identyfikuje osobę fizyczną;
4. Administrator w formularzu oceny skutków ryzyka przypisał ocenę 5 w skali od 0 do 21, która to klasyfikowała ww. zdarzenie jako „średnio dotkliwe", uzasadniając, że „Osoby fizyczne zostaną dotknięte naruszeniem w stopniu średnim, tj.: mogą napotkać pewne niedogodności, które są łatwe do przezwyciężenia (czas spędzony na ponownym wejściu w informacje, rozdrażnienie, irytacja itp.). Niemniej naruszenie ochrony danych nie wywiera znaczących skutków dla praw i obowiązków

osoby której dane dotyczą.” - uzależnianie reakcji na zaistniałe naruszenie od ziszczenia się jego potencjalnych konsekwencji jest sprzeczne z zasadą, zgodnie z którą administrator ma przeciwdziałać konsekwencjom naruszenia lub minimalizować jego negatywne skutki;

5. Możliwe konsekwencje zaistniałego zdarzenia nie muszą się zmaterializować - samo wystąpienie naruszenia ochrony danych osobowych, z którym wiąże się ryzyko naruszenia praw lub wolności osób fizycznych, implikuje obowiązek zgłoszenia naruszenia właściwemu organowi nadzorczemu (art. 33 ust. 1 RODO);
6. Możliwość wykorzystania danych do wyłudzenia kredytu lub pożyczki, jako powodujące powstanie straty finansowej, stanowi o wysokim ryzyku naruszenia praw lub wolności osób fizycznych;
7. Przy dokonywaniu analizy ryzyka nie należy w sposób arbitralny obniżać poziomu tego ryzyka w sytuacji, gdy naruszenie dotyczy tylko jednej osoby, ponieważ naruszenie może mieć poważne konsekwencje nawet dla jednej osoby;
8. Oceny ryzyka naruszenia praw lub wolności osoby fizycznej należy dokonać z punktu widzenia interesów osoby dotkniętej naruszeniem, a nie interesów administratora;
9. Przyjęcie przez Administratora zaniżonych wartości w formularzu oceny ryzyka miała kluczowy wpływ na finalną ocenę poziomu ryzyka naruszenia praw lub wolności osoby fizyczne;
10. Opisane naruszenia jednocześnie naruszenie tajemnicy lekarskiej - powyższa okoliczność dodatkowo przesądza o zasadności przyjęcia, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osoby fizycznej dotkniętej tym naruszeniem;

Kontakt :

W przypadku dodatkowych pytań, zachęcamy do bezpośredniego kontaktu z naszą ekspertką.

Anna Matusiak-Wekiera
Radca prawny

Head of Data Protection/Compliance Practice
anna.matusiak-wekiera@jdp-law.pl