Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Szwecja

Data Protection Authority of Sweden (Integritetsskyddsmyndigheten)

Data wydania decyzji

07.06.2021 r.

Podmiot kontrolowany

MedHelp AB

Wysokość kary

1 200 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 5 (1) a), f) RODO, Art. 6 RODO, Art. 9 (1) RODO, Art. 13 RODO, Art. 32 RODO
Nieprzestrzeganie ogólnych zasad przetwarzania danych

Przedmiot decyzji

Źródło postępowania:

W lutym 2019 roku Computer Sweden opublikował artykuł ujawniający niechroniony dostęp do nagrań rozmów telefonicznych z numerem infolinii 1177. Pliki znajdowały się na otwartym serwerze www, niezabezpieczonym hasłem ani innymi środkami utrudniającymi ujawnienie zawartości.

Opis wydarzeń:

1) W związku z doniesieniami medialnymi, w marcu 2019 roku szwedzki organ nadzorczy wszczął postępowanie kontrolne mające na celu ustalenie stanu faktycznego.

2) W trakcie czynności kontrolnych ustalono, iż:
a) MedHelp AB (MedHelp) udziela porad zdrowotnych osobom dzwoniącym pod numer 1177, a tym samym jest administratorem ich danych;
b) MedHelp nawiązała współpracę z tajlandzką firmą MediCall, która jako podwykonawca udzielała porad zdrowotnych osobom dzwoniącym pod numer 1177;
c) MediCall podczas rozmów telefonicznych zbierała dane osobowe oraz wprowadzała je do systemu dokumentacji medycznej MedHelp;
d) MedHelp odbierała rocznie około 3 milionów połączeń, spośród których 80% kierowanych było do MedHelp, a pozostałe 20% do MediCall;
e) MedHelp powzięło informacje o naruszeniu bezpieczeństwa danych osobowych od wiceprezesa Inera AB;
f) naruszenie dotyczyło pacjentów i pracowników MediCall;
g) dane osobowe objęte naruszeniem obejmowały: informacje o stanie zdrowia, życiu seksualnym, numer ubezpieczenia społecznego, datę urodzenia, informacje identyfikujące, takie jak imię i nazwisko oraz dane kontaktowe;
h) w momencie wykrycia naruszenia na serwerze pamięci masowej Voice NAS znajdowało się 2,7 mln plików audio z nagraniami rozmów, które odpowiadają liczbie między 650 000 a 900 000 połączeń;
i) w związku z naruszeniem MedHelp podjął decyzję o przeniesieniu danych z Voice NAS na własne serwery oraz usunięciu danych z serwerów Voice NAS.

3) Szwedzki organ nadzorczy dopatrzył się następujących naruszeń:
a) MediCall przetwarzała dane osobowe bez stosowania się do szwedzkiego systemu prawnego oraz bez ustawowego obowiązku zachowania poufności;
b) brak skutecznej procedury regularnego testowania i badania oraz oceny skuteczności środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych;
c) brak realizacji obowiązku informacyjnego oraz poinformowania o przekazywaniu danych do państwa trzeciego;
d) brak wykonywania kopii zapasowych plików audio, zawierających nagrane rozmowy.

Przyczyna naruszenia:

Administrator nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja Data Protection Authority of Sweden (Integritetsskyddsmyndigheten):

1) Kara pieniężna w wysokości 12 000 000 SEK (1 200 000 EUR), w tym:
a) 3 000 000 SEK za ujawnienie danych osobowych tajlandzkiej firmie MediCall oraz umożliwienie jej zbierania danych osobowych;
b) 8 000 000 SEK za przechowywanie danych osobowych w plikach audio z nagranymi rozmowami telefonicznymi na serwerze pamięci masowej Voice NAS, bez zastosowania adekwatnych środków technicznych i organizacyjnych, zapewniających odpowiedni poziomu bezpieczeństwa danych;
c) 500 000 SEK za brak realizacji obowiązku informacyjnego;
d) 500 000 SEK za brak kopii zapasowych plików audio z nagranymi rozmowami.

2) W terminie nieprzekraczającym dwóch miesięcy od uprawomocnienia się decyzji, administrator został zobowiązany do podjęcia następujących środków:
a) realizacji obowiązku informacyjnego wobec osób dzwoniących pod numer 1177;
b) wykonywania kopii zapasowych plików audio z nagranymi rozmowami, zgodnie z zaplanowaną częstotliwością, przechowywania danych w sposób zapewniający bezpieczeństwo wraz z określeniem okresu czasu ich przechowywania oraz ustalenia harmonogramu przeprowadzania testów ponownego odczytu nagrań.

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) Dokonuj weryfikacji doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceniaj weryfikację przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

3) Realizuj obowiązek informacyjny, który w sposób jasny i precyzyjny będzie informował osoby, których dane dotyczą, o przetwarzaniu ich danych osobowych. Staraj się używać prostego języka, unikać zdań i skomplikowanych struktur językowych. Istotne jest również to, aby cele i podstawa prawna przetwarzania danych osobowych były łatwe do zrozumienia.

4) Wykonuj kopie zapasowe na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych. Pamiętaj, aby zaplanować harmonogram wykonywania kopii zapasowych oraz określić okres ich przechowywania. Nie zapomnij o testowaniu możliwości odtworzenia kopii zapasowych.

5) Zabezpiecz serwer, na którym przechowujesz dane w taki sposób, aby osoby nieuprawnione nie miały do nich dostępu.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak