STUDIUM PRZYPADKU

Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Data wydania decyzji
08.09.2020 r.

Podmiot kontrolowany
Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

Wysokość kary
50 000 PLN

Rodzaj naruszenia

Naruszenie Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie (SGGW) zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych naruszenie ochrony danych osobowych kandydatów na studia w SGGW, które miało miejsce w listopadzie 2019 r. i związane było z kradzieżą przenośnego prywatnego komputera pracownika SGGW. Przedmiotowe naruszenie dotyczyło około 81 624 kandydatów na studia wpisanych do Systemu Obsługi Kandydatów (SOK) z okresu ostatnich 5 lat.

W listopadzie 2019 roku pracownicy Urzędu Ochrony Danych Osobowych (UODO) dokonali czynności kontrolnych i ustalili, iż naruszenie związane było z kradzieżą przenośnego prywatnego komputera pracownika SGGW, pełniącego również funkcję sekretarza Uczelnianej Komisji Rekrutacyjnej SGGW. Skradziony laptop był używany przez ww. pracownika do celów prywatnych i służbowych, w tym również do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych w ramach pełnionej przez tą osobę funkcji. Pracownik importował na swój prywatny komputer z SOK pełny zestaw danych osobowych kandydatów na studia. SGGW nie posiadała informacji o tym fakcie, a operacja eksportu danych nie była rejestrowana w SOK.

Kompas FORSAFE

PUODO zwrócił uwagę na następujące zagadnienia:

DOKUMENTACJA

- Opracowanie polityki ochrony danych rozumianej jako strategia ochrony danych, plan działań mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych.
- Wdrożenie procedury wykorzystywania sprzętu prywatnego do celów służbowych.
- Wdrożenie procedury retencji danych.
- Wdrożenie procedury zgłaszania naruszeń bezpieczeństwa danych osobowych.
- Uwzględnienie w polityce ochrony danych planu utrzymania zgodności oraz prowadzenia audytów wewnętrznych, w tym m.in. zasad monitorowania i audytu procedur wewnętrznych.
- Opracowanie metodyki analizy ryzyka.

CZYNNOŚCI

- Zapewnienie ochrony danych osobowych na płaszczyźnie nie tylko formalnej (dokumentacja), ale i praktycznej.
- Wykonywanie przeglądów i aktualizacji dokumentacji opisującej system ochrony danych osobowych w szczególności w sytuacji zmian w przepisach o ochronie danych osobowych.
- Monitorowanie procedur związanych z ochroną danych osobowych oraz dostosowywanie ich do procesów przetwarzania danych.
- Monitorowanie, weryfikacja i kontrola nad sposobem i zakresem przetwarzania danych osobowych.
- Weryfikacja procesów przetwarzania danych osobowych w aspekcie retencji danych.
- Usunięcie danych lub ich anonimizacja po osiągnięciu celów przetwarzania.
- Prowadzenie rejestru czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 1 Rozporządzenia.
- Uwzględnienie informacji o odbiorcy danych w rejestrze czynności przetwarzania danych osobowych.
- Cykliczne monitorowanie zawartości rejestru czynności przetwarzania danych osobowych.
- Wykonywanie analizy ryzyka dla procesów przetwarzania danych osobowych z uwzględnieniem: terminu jej wykonania, informacji o osobie wykonującej analizę ryzyka, informacji o terminie zatwierdzenia oraz osobie zatwierdzającej analizę ryzyka.

ŚRODKI TECHNICZNE I ORGANIZACYJNE

- Wdrożenie środków technicznych zabezpieczających komputery przenośne przed nieuprawnionym dostępem.
- Wdrożenie środków technicznych zabezpieczających pliki z danymi osobowymi przed nieuprawnionym dostępem.
- Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
- Wdrożenie środków takich jak zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.
- Przeanalizowanie systemów informatycznych i aplikacji pod kątem rozliczalności.
- Zastosowanie zasady rozliczalności w systemach informatycznych realizowanej w formie automatycznie generowanych zapisów (tzw. logów) zawierających określony zestaw informacji umożliwiający stwierdzenie kto, kiedy, jakie operacje oraz w odniesieniu do jakich danych wykonał w systemie.
- Weryfikacja programów i aplikacji w zakresie rejestrowania eksportu danych oraz zakresu eksportowanych danych.

ROLA INSPEKTORA OCHRONY DANYCH

- Ustalenie przez Inspektora Ochrony Danych priorytetów w swojej pracy, które powinny polegać na indywidualnym i samodzielnym określaniu środków oraz metod działania i dostosowywania ich do specyfiki konkretnego administratora.
- Wykonywanie zadań przez Inspektora Ochrony Danych z uwzględnieniem należytego ryzyka związanego z operacjami przetwarzania danych osobowych.
- Przeprowadzanie audytów przez Inspektora Ochrony Danych, obejmujących następujące etapy: zbieranie informacji, analizowanie i sprawdzanie zgodności przetwarzania, informowanie, doradzanie i rekomendowanie określonych rozwiązań.
  Etap zbierania informacji powinien uwzględniać zbieranie informacji o podmiocie i stosowanych w nim procesach przetwarzania danych, w tym identyfikacja czynności przetwarzania danych, ustalenie aktywów wykorzystywanych do przetwarzania danych, tj. systemów informatycznych, dokumentów, nośników danych i ustalenie zakresów danych, które są przetwarzane wraz z ich kategoryzacją.
  Etap analizowania i sprawdzania zgodności przetwarzania z przepisami rozporządzenia 2016/679 powinien być wykonany pod względem formalnoprawnym, jak i zgodności systemów informatycznych.
  Etap informowania, doradzania i rekomendowania określonych rozwiązań powinien być zakończony opracowaniem raportu, w którym wskazane są rekomendacje.
- Monitorowanie przepisów o ochronie danych osobowych przez Inspektora Ochrony Danych.
- Dostosowanie szkoleń realizowanych przez Inspektora Ochrony Danych do specyfiki podmiotu oraz specyfiki poszczególnych działów/wydziałów.
- Zapewnienie Inspektorowi Ochrony Danych szkoleń podnoszących jego kwalifikacje, monitorowanie procesu szkolenia, w tym dysponowanie potwierdzeniem odbycia szkolenia przez Inspektora Ochrony Danych.
- Włączanie Inspektora Ochrony Danych we wszystkie sprawy dotyczące ochrony danych osobowych.
- Wyznaczenie Inspektora Ochrony Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań związanych z ochroną danych osobowych.
- Unikanie częstej zmiany Inspektora Ochrony Danych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak