Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **11.02.2021 r.**

Podmiot kontrolowany: **Krajowa Szkoła Sądownictwa i Prokuratury w Krakowie**

Wysokość kary: **100 000 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 5 (1) f), Art. 25 (1), Art. 28 (3), Art. 32 (1), (2) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W kwietniu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja od Krajowej Szkoły Sądownictwa i Prokuratury (KSSiP) o naruszeniu ochrony danych osobowych, które polegało na ujawnieniu danych ze strony internetowej platformy szkoleniowej.

Opis wydarzeń:

1) KSSiP został powiadomiony przez Komendę Główną Policji o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl.

2) Administrator zapoznał się z rodzajem danych i ustalił, że są to dane z bazy danych witryny szkolenia.kssip.gov.pl, która powstała w lutym 2020 r. w trakcie testowej migracji do nowej platformy szkoleniowej ekssip.kssip.gov.pl.

3) Naruszenie dotyczyło danych osobowych 50 283 osób.

4) Naruszenie obejmowało dane osobowe: sędziów, asesorów sądowych, prokuratorów i asesorów prokuratury, referendarzy sądowych, asystentów sędziów, asystentów prokuratorów, kuratorów zawodowych oraz urzędników sądów i prokuratury. Na platformie szkoleniowej KSSiP znajdowały się również konta części wykładowców prowadzących szkolenia ustawiczne, nielicznych aplikantów KSSiP oraz osób, których konta aktywowano na podstawie indywidualnych decyzji.

5) Kategorie danych, których dotyczy naruszenie obejmowały: imię i nazwisko, adres e-mail, nazwa użytkownika, numer telefonu, jednostka, wydział, adres jednostki, miejscowość, dane o charakterze technicznym: adres IP, data pierwszego i ostatniego logowania, hasło (w postaci niejawnej). W 44 262 przypadkach rekordy zawierały również numer PESEL.

6) KSSiP w celu zminimalizowania negatywnych skutków dla osób, których dane dotyczą:

a. wysłał żądanie zablokowania udostępniania oraz pobierania tych informacji do administracji forum publikującego odnośnik do bazy oraz do administracji portalu udostępniającego plik z danymi,

b. usunął wszystkie hasła na nowej platformie i umieścił informację o konieczności zmiany hasła przy logowaniu do nowej platformy,

c. poinformował drogą mailową wszystkie osoby, których dotyczyło naruszenie o zaistniałej sytuacji,

d. poinformował na stronie www o naruszeniu bezpieczeństwa danych osobowych.

7) Prezes UODO stwierdził, że KSSiP naruszył RODO poprzez:

a. niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania,

b. brak testowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej,

c. niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania,

d. powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu:
- bez umownego zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora,
- bez określenia w umowie powierzenia przetwarzania danych osobowych kategorii osób,
- bez doprecyzowania rodzaju danych osobowych przez wskazanie ich kategorii.

Przyczyna naruszenia:

KSSiP nie podjęła wystarczających działań mających na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu. Nie zweryfikowała również czy we wskazanej przez KSSiP lokalizacji nadal znajduje się kopia bazy danych.

Decyzja PUODO:

1) Kara pieniężna w wysokości 100 000 PLN

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 regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

3) Dokonując oceny proporcjonalności zabezpieczeń weź pod uwagę czynniki i okoliczności dotyczące przetwarzania (np. rodzaj, sposób przetwarzania danych) i ryzyko, jakie się z nim wiąże.

4) Zawierając umowę powierzenia uwzględnij w niej zapisy o:

a. przedmiocie i czasie trwania przetwarzania,

b. charakterze i celu przetwarzania,

c. rodzaju danych osobowych,

d. kategorii osób, których dane dotyczą,

e. obowiązkach i prawach administratora,

f. zobowiązaniu osób upoważnionych do przetwarzania danych osobowych do zachowania poufności,

g. uprawnieniu do przeprowadzania audytów, w tym inspekcji.

5) Weryfikuj czy podmiot przetwarzający wywiązał się ze zlecenia usunięcia danych ze wskazanej lokalizacji. Pamiętaj, że obowiązkiem administratora jest weryfikacja, czy zlecona czynność została wykonana.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak