JDP

Newsletter

Orzeczenia w sprawie ochrony danych osobowych

_case study 3.0

12 października 2022

_case study 3.0

Niezrealizowanie obowiązków ciążących na administratorze, wynikających z RODO.

Analiza

- Sygnatura: **II SA/Wa 1384/21**
- Data: dnia **26 stycznia 2022 r.**
- Organ: **Wojewódzki Sąd Administracyjny w Warszawie**
- Administrator: **Krajowa Szkoła Sądownictwa i Prokuratury (KSSIP)**
- Wysokość kary: **100 000 zł**
- Decyzja UODO: **DKN.5130.2024.2020 z dnia 11 lutego 2021 r.**

Czy jako administrator danych osobowych stosujesz wzór umowy powierzenia danych osobowych zgodny z RODO? Czy informujesz pracowników, których wyznaczyłeś w umowie powierzenia do kontaktu o wynikających z tego obowiązkach? Wojewódzki Sąd Administracyjny w Warszawie podtrzymał w mocy decyzję Prezesa UODO, która nakładała na Krajowa Szkoła Sądownictwa i Prokuratury (KSSIP) karę w wysokości 100 000 zł.

_case study 3.0

Rodzaj naruszenia

Niezrealizowanie obowiązków ciążących na administratorze, wynikających z RODO, poprzez:

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

b) brak przetestowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej KSSiP a tym samym niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania;

c) powierzenie przetwarzania danych osobowych spółce trzeciej z naruszeniem art. 28 ust. 3 RODO, tj. bez umownego zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, a także bez określenia w umowie powierzenia przetwarzania danych osobowych kategorii osób oraz bez doprecyzowania rodzaju danych osobowych przez wskazanie ich kategorii.

_case study 3.0

Opis naruszenia

KSSIP został powiadomiony przez Komendę Główną Policji o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl. Naruszenie dotyczyło danych z bazy danych witryny szkolenia.kssip.gov.pl powstałe w trakcie testowej migracji do nowej platformy szkoleniowej ekssip.kssip.gov.pl. Naruszenie dotyczyło danych osobowych 50 283 osób. Kategorie danych obejmują: 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), a także numery ewidencyjne PESEL.

_case study 3.0

Prezes UODO w decyzji wskazał

1. Treść umowy powierzenia ze spółką e. Sp. z o.o. w sposób niewystarczający:
   a) doprecyzowuje zakres powierzanych danych - KSSIP nie wskazała kategorii osób, których dane dotyczą oraz nie doprecyzowała rodzaju danych osobowych przez wskazanie ich kategorii;
   b) zobowiązuje podmiot przetwarzający do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora – umowa powierzenia przetwarzania danych stanowi musi stanowić, że podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora.
   c) umowa powierzenia powinna zawierać przynajmniej ogólne sformułowanie zobowiązujące podmiot przetwarzający do działania wyłącznie na udokumentowane polecenie administratora;
2. W ww. umowach powierzenia przetwarzania danych wskazuje się, że powierzone dane osobowe będą przetwarzane wyłącznie w celu realizacji umowy głównej, tj. wykonywania na dedykowanych serwerach, dostarczanych przez e., usługi hostingu strony www oraz platformy szkoleniowej, hostingu poczty elektronicznej, a także zapewnienie pełnej obsługi administracyjnej dla ww. serwerów na zasadach opisanych w umowie głównej; Pomimo tych zapisów oczekiwano wykonania zadań wykraczających poza zakres tej umowy;

_case study 3.0

Prezes UODO w decyzji wskazał

6. Jakiekolwiek zmiany w procesie przetwarzania danych osobowych są okolicznością szczególnie obarczającą administratora odpowiedzialnością za zmaterializowanie się zagrożeń związanych z niedopełnieniem powyższych obowiązków. Zapewnienie odpowiedniego bezpieczeństwa danym osobowym, na każdym etapie przetwarzania, powinno być przedmiotem szczególnej troski administratora;
7. Wybór dającego gwarancję odpowiednich zabezpieczeń podmiotu przetwarzającego jest obowiązkiem administratora.

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