Zgubienie pendrive – pracodawca nie może winić pracownika za wyciek danych

Kategoria: Aktualności
Opublikowano: piątek, 04, październik 2024 10:12
Patrycja Grebla-Tarasek
Odsłony: 883

W 2020 roku kurator sądowy zgubił niezaszyfrowanego pendrive'a z danymi osobowymi 400 osób. Były tam: imiona i nazwiska, daty urodzenia, adresy zamieszkania lub pobytu, numery PESEL, dane o zarobkach i majątku, numery dowodów osobistych, telefonów, dane o zdrowiu i wyrokach skazujących.

Prezes Sądu Rejonowego – administrator danych, zgłosił to naruszenie ochrony danych do Prezesa UODO i poinformował o nim osoby, których dane znajdowały się na zgubionym nośniku. PUODO po analizie stwierdził, że administrator nie wypełnił tego obowiązku prawidłowo: nie poinformował odpowiednio o możliwych konsekwencjach naruszenia ochrony danych osobowych oraz o tym, co zrobił administrator, by zminimalizować skutki naruszenia.

Prezes UODO ustalił, że administrator niewłaściwie wdrożył zabezpieczenia techniczne i organizacyjne. Otóż zgodnie z procedurami funkcjonującymi w sądzie obowiązek zabezpieczenia służbowego nośnika zawierającego dane osobowe spoczywał na samych pracownikach. Obowiązek ewidencjonowania i szyfrowania nośników został zaś wprowadzony dopiero po tym, jak kurator zgubił swój pendrive.

Wcześniej pracownicy zostali po prostu przeszkoleni w zakresie ochrony danych. Tymczasem, jak zauważył Prezes UODO**, jednorazowe szkolenie nie wystarczy. Nie gwarantuje, że pracownik nie będzie przenosić danych na niezabezpieczonym nośniku.** W omawianym przypadku pracownik chronił dane nosząc pendrive w zamykanej torbie.

W niniejszej sprawie administrator:

- nie zrobił odpowiedniej analizy ryzyka, więc nie mógł we właściwy sposób dążyć do jego minimalizacji;
- ograniczył się do zabezpieczeń organizacyjnych (procedury, szkolenia), nie weryfikując ich skuteczności;
- nie wdrożył zaś zabezpieczeń technicznych takich jak szyfrowanie, czy sprawdzanie nośników.

Wszystko to było nieadekwatne wobec ryzyka utraty lub zniszczenia tych danych. Zarówno w zakresie prawdopodobieństwa takiego zdarzenia jak i jego konsekwencji.

Administratorzy, przetwarzając dane osobowe, muszą doprowadzić do tego, by procesy przetwarzania danych były zgodne z RODO. W tym celu powinni wdrożyć organizacyjne i techniczne środki bezpieczeństwa. Tymczasem w przedmiotowej sprawie administrator ograniczył się do wydania niezabezpieczonych nośników pamięci oraz zobowiązania kuratorów sądowych do wdrożenia zabezpieczeń tej pamięci we własnym zakresie. To nie wystarczyło, bo w przypadku zgubienia nośnika dostęp do danych mogły zyskać osoby nieuprawnione.

Źródło: UODO