# Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **9 grudnia 2021 r.**

Podmiot kontrolowany: **Politechnika Warszawska**

Rodzaj kary: **45 000 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

## Rodzaj naruszenia

Naruszenie art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

## Przedmiot decyzji

**Źródło postępowania**:

W maju 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Politechniki Warszawskiej (Uczelnia) polegające na pobraniu z zasobów sieci informatycznej Uczelni, przez osobę nieznaną i nieuprawnioną, bazy danych zawierającej dane osobowe studentów i wykładowców studiów z lat 2008-2020 oraz 169 kandydatów na studia na rok akademicki 2019/2020.

**Opis wydarzeń:**

**1)** Do naruszenia doszło na skutek zalogowania się przez osobę nieuprawnioną do systemu informatycznego Uczelni, która wykorzystała do tego celu dane uwierzytelniające wykładowcy.

**2)** W kolejnym kroku osoba nieuprawniona umieściła w systemie informatycznym plik typu backdoor, który umożliwił jej pobranie baz z danymi osobowymi.

**3)** W wyniku zaistniałej sytuacji administrator systemu podjął decyzję o odłączeniu serwera od sieci publicznej oraz o całkowitym wyłączeniu systemu informatycznego z użytku.

**4)** Naruszenie łącznie dotyczyło danych osobowych 5013 osób.

**5)** Kategorie danych, których dotyczyło naruszenie obejmowały: imię i nazwisko, imiona rodziców, datę urodzenia, adres zamieszkania lub pobytu, numer PESEL, adres e-mail, nazwę użytkownika i/lub hasło, nazwisko rodowe matki, serię i numer dowodu osobistego oraz numer telefonu.

**6)** Prezes UODO w związku z wszczętym postępowaniem administracyjnym ustalił, iż Uczelnia:

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

**b)** nie dokonywała regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,

**c)** nie uwzględniła we właściwy sposób ryzyka związanego z przetwarzaniem danych osobowych w systemie informatycznym,

**d)** nie uwzględniła ryzyka związanego z przetwarzaniem w aplikacji haseł użytkowników w postaci funkcji skrótu MD5 bez dodatkowego losowego parametru funkcji szyfrowania,

**e)** nie wykonała formalnej analizy ryzyka,

**f)** nie dokonała analizy zasadności 4-tygodniowego przechowywania logów maszyny wirtualnej, na której znajdował się system informatyczny,

**g)** nie dokonała analizy zasadności braku szczegółowego dziennika zdarzeń w aplikacji,

**h)** nie wdrożyła odpowiednich środków technicznych i organizacyjnych, zapewniających utrzymanie zdolności do szybkiego i skutecznego stwierdzenia wystąpienia naruszenia,

**i)** nie wykonywała testów penetracyjnych aplikacji pozwalających na wykrycie podatności systemu na ataki z sieci publicznej.

**Przyczyna naruszenia**:

Uczelnia nie zastosowała adekwatnych środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym.

**Decyzja PUODO**:

Kara pieniężna w wysokości 45 000 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)** Dokonaj wdrożenia procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego.

**4)** Przeprowadzaj testy nastawione na weryfikację zabezpieczeń programów i aplikacji, w tym testy podatności/penetracyjne.

**5)** Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

**6)** Wykonując analizę ryzyka i identyfikując zagrożenia uwzględnij: zakres przetwarzanych danych, liczbę użytkowników aplikacji, charakter ich uprawnień, uwarunkowania środowiska informatycznego, w którym aplikacja funkcjonuje, możliwości wpływu osób trzecich, które w sposób nieuprawniony uzyskują dostęp do aplikacji.

**7)** Wykonując analizę ryzyka potencjalnego ataku uwzględnij: metody socjotechniczne, stan wiedzy technicznej, fizyczne aspekty bezpieczeństwa, w tym bezpieczeństwa teleinformatycznego, analizę atakującego z punktu widzenia osoby nieznającej organizacji administratora oraz jej infrastruktury informatycznej, jak również osoby, która wiedzę tę posiada.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne Katarzyna Cieślak