Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **16 maja 2023 r.**

Podmiot kontrolowany **Burmistrz Miasta Z.**

Wysokość kary **30 000 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

W czerwcu 2022 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Burmistrza Miasta Z. (Burmistrz) polegające na zablokowaniu dostępu do serwera.

Opis wydarzeń:

1. Burmistrz w wysłanym zgłoszeniu poinformował, iż naruszenie:

a) dotyczyło około 9400 osób,

b) obejmowało następujące dane osobowe – imię i nazwisko, imiona rodziców, data urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer PESEL, adres e-mail, dane dotyczące zarobków i/lub posiadanego majątku, nazwisko rodowe matki, numer telefonu, wizerunek.

2. Na podstawie zebranego materiału dowodowego Prezes UODO ustalił, że:

a) naruszenie ochrony danych osobowych zostało spowodowane atakiem ransomware na skutek wykorzystania podatności istniejącej w systemie teleinformatycznym,

b) podatnością systemu informatycznego wykorzystaną do przeprowadzania ataku była niezaktualizowana baza danych wirusów,

c) wszystkie dane zostały odzyskane z kopii zapasowych oraz dokumentacji papierowej,

d) serwer, na którym były przetrzymywane kopie zapasowe, uległ awarii a pozostałe kopie zapasowe zostały zaszyfrowane,

e) przeprowadzona analiza ryzyka uwzględniała zaistniałe ryzyka, ale wskazywała na małe prawdopodobieństwo ich materializacji,

f) nie przewidziano procedur tworzenia kopii zapasowych,

g) nie był wykonywany regularny backup serwerów, aplikacji, plików, konfiguracji,

h) nie były przeprowadzane testy możliwości odtworzenia kopii,

i) na serwerze był zainstalowany system operacyjny, który stracił wsparcie producenta.

3. W ocenie Prezesa UODO przyczyną wystąpienia naruszenia ochrony danych osobowych była nierzetelnie przeprowadzona analiza ryzyka oraz niepełne wdrożenie środków technicznych i organizacyjnych gwarantujących bezpieczeństwo w procesie przetwarzania danych osobowych.

Przyczyna naruszenia:

Burmistrz nie dokonał adekwatnego doboru zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz nie realizował odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych.

Decyzja PUODO:

1. Kara pieniężna w wysokości 30 000 PLN.

2. Nakaz dostosowania operacji przetwarzania poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania – w terminie 30 dni od dnia doręczenia decyzji.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.56.2022

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 przetwarzania danych osobowych w systemach teleinformatycznych.

3. Wykonuj kopie zapasowe na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych oraz weryfikuj je pod kątem możliwości ich odtworzenia.

4. Do przetwarzania danych osobowych wykorzystuj oprogramowanie posiadające aktualne wsparcie techniczne producenta.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska