Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

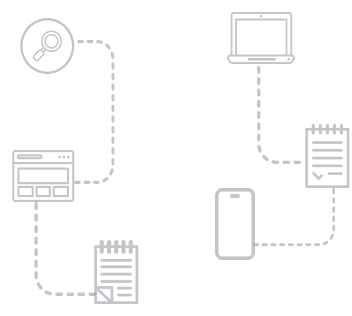
FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Data wydania decyzji

17.12.2020 r.

Podmiot kontrolowany

ID Finance Poland Sp. z o.o. w likwidacji



Wysokość kary

1 069 850 PLN

Rodzaj naruszenia

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

Przedmiot decyzji

W marcu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja o naruszeniu ochrony danych osobowych, polegającym na nieautoryzowanym dostępie do danych osobowych 140 699 klientów i potencjalnych klientów, którzy przeszli przez proces rejestracji w serwisie internetowym moneyman.pl. Powodem zaistniałej sytuacji było błędne działanie serwera związane z jego restartem wykonanym przez IDFT Sp. z o.o. - podmiot odpowiedzialny za realizację usług mających charakter hostingu. W trakcie restartu serwera doszło do zresetowania ustawień oprogramowania odpowiadającego za bezpieczeństwo serwera i w konsekwencji dane osobowe znajdujące się na serwerze stały się publicznie dostępne. Wykorzystując tą sytuację nieustalony podmiot trzeci pobrał znajdującą się na tym serwerze bazę danych, a następnie ją z niego usunął. Wszedł w posiadanie takich danych jak: imię i nazwisko, poziom wykształcenia, adres e-mail, dane dotyczące zatrudnienia, adres e-mail osoby, której klient chce polecić pożyczkę, dane dotyczące zarobków, dane dotyczące stanu cywilnego, numer telefonu (stacjonarnego, komórkowego, wcześniej używanego numeru telefonu), numer PESEL, narodowość, numer NIP, hasło, miejsce urodzenia, adres korespondencyjny, adres zameldowania, numer telefonu do miejsca pracy oraz numer rachunku bankowego. Ostatecznie wspomniany podmiot zwrócił się do Spółki z żądaniem zapłaty wynagrodzenia w zamian za zwrot pozyskanej bazy danych.
W związku ze zgłoszonym naruszeniem pracownicy UODO dokonali w Spółce kontroli i na podstawie zgromadzonych informacji i dowodów ustalili, że Spółka nie wdrożyła zarówno w fazie projektowania procesu przetwarzania jak i w czasie samego przetwarzania, odpowiednich środków technicznych i organizacyjnych odpowiadających ryzyku naruszenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemu przetwarzania danych osobowych, a także zapewniających zdolność skutecznego i szybkiego stwierdzenia naruszenia ochrony danych osobowych oraz zapewniających regularną ocenę skuteczności tych środków. Brak tych działań skutkowało uzyskaniem przez osoby trzecie nieuprawnionego dostępu do przetwarzanych danych osobowych.

Kompas FORSAFE

JAK ZAPOBIEGAĆ TAKIM NARUSZENIOM?

1) Swoje działania opieraj na podejściu proaktywnym i prewencyjnym polegającym na zapewnianiu bezpieczeństwa danym osobowym na każdym etapie ich przetwarzania.

2) 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.

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

4) Wykonując restart serwera pamiętaj, by sprawdzić prawidłowość konfiguracji zabezpieczeń.

5) Przechowuj hasła w systemach informatycznych w postaci niejawnej (np. poprzez zastosowanie funkcji skrótu, zwanej też haszowaniem), aby zapewnić poufność hasła i ograniczyć jego znajomość wyłącznie do osoby, która się nim posługuje.

6) Opracuj i wdróż procedury zgłaszania naruszeń bezpieczeństwa danych osobowych, które będą uwzględniały kwestie związane ze sprawnym i szybkim stwierdzeniem naruszenia ochrony danych.

7) Nie ignoruj informacji o potencjalnym naruszeniu ochrony danych osobowych otrzymanych od osoby fizycznej lub z innego źródła. Każdy sygnał o ewentualnych nieprawidłowościach powinien być przedmiotem wnikliwej analizy.

8) W sytuacji wystąpienia naruszenia ochrony danych osobowych wykonaj jego ocenę pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

9) Wykonaj analizę ryzyka, gdy w związku z naruszeniem ochrony danych osobowych zostanie ujawnione ryzyko nie rozpatrywane we wcześniejszej analizie.

10) Zawierając umowę powierzenia uwzględnij w niej zapisy odnoszące się do postępowania w sytuacji, gdy doszło do naruszenia bezpieczeństwa danych osobowych, ale również do sytuacji jego potencjalnego wystąpienia.

11) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak