Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **08 luty 2023 r.**

Podmiot kontrolowany: **K. P. prowadząca działalność gospodarczą**

Wysokość kary: **33 012 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1, art. 28 ust. 1 i 3, art. 32 ust. 1 i 2 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W grudniu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od K. P. prowadzącej działalność gospodarczą (Przedsiębiorca) polegające na utracie poufności danych w związku z działaniem wirusa komputerowego

Opis wydarzeń:

1) Przedsiębiorca w wysłanym zgłoszeniu poinformował, iż:

a) podmiotem uczestniczącym w przetwarzaniu danych osobowych, których dotyczy naruszenie jest M. H. prowadzący działalność gospodarczą (ASI) jako podmiot zajmujący się obsługą informatyczną,

b) naruszenie dotyczyło ok. 800 osób – byłych i obecnych klientów Przedsiębiorcy,

c) zakres naruszenia obejmował następujące dane – imię, nazwisko, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, adres e-mail, numer telefonu.

2) Prezes UODO zwrócił się do Przedsiębiorcy o złożenie dodatkowych wyjaśnień w przedmiotowej sprawie, gdyż z doniesień opisanych na jednym z portali internetowych wynikało, iż w tym samym czasie doszło do naruszenia ochrony danych osobowych znajdujących się m.in. w polisach ubezpieczeniowych zawieranych w okresie od maja 2015 r. do listopada 2020 r. z różnymi towarzystwami ubezpieczeniowymi, które były publicznie dostępne na zasobach informatycznych. Wśród ujawnionych plików miały znajdować się również dokumenty takie jak: wyniki badań onkologicznych, kopie umów i polis ubezpieczeniowych z danymi klientów, zdjęcia pojazdów wykonywane do celów ubezpieczeniowych, dokumenty z audytu bezpieczeństwa danych osobowych, polityka bezpieczeństwa, a także plik z danymi dostępowymi do zasobów sieciowych.

3) W odpowiedzi na powyższe pismo, Przedsiębiorca potwierdził, iż wysłane przez niego zgłoszenie dotyczy tego samego zdarzenia, które zostało opisane na portalu internetowym.

4) Ponadto Przedsiębiorca dołączył zgłoszenie uzupełniające, w którym wskazał, że:

a) w wyniku infekcji wirusem doszło do upublicznienia dokumentów, co zostało niezwłocznie zablokowane po powzięciu o tym informacji,

b) naruszenie rozpoczęło się w listopadzie 2020 r. i dotyczyło 2494 osób, których dane znajdowały się w folderze roboczym udostępnionym w sieci lokalnej dla pracowników Przedsiębiorcy,

c) zakres naruszenia obejmował następujące dane – imię, nazwisko, adres zamieszkania lub pobytu, numer PESEL, adres e-mail, numer telefonu, seria i numer dowodu osobistego, dane dotyczące zdrowia,

d) uruchomił stronę internetową, na której zamieścił komunikat o naruszeniu,

e) prawdopodobną przyczyną zdarzenia było działanie hakerskie polegające na nielegalnym wejściu w posiadanie loginów oraz haseł używanych do konfiguracji serwerów.

5) Przedsiębiorca zlecił również firmie zewnętrznej audyt systemu informatycznego, który wykazał, że powodem zdarzenia była błędna konfiguracja serwerów dokonana przez ASI podczas wdrożenia pracy zdalnej.

6) Audyt wykazał również, że przedsiębiorca miał wdrożone przez ASI stosunkowo niskie poziomy zabezpieczeń technicznych i organizacyjnych.

7) Biorąc pod uwagę zaistniałą sytuację, Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Przedsiębiorcę administracyjnej kary pieniężnej.

8) Na podstawie zebranego materiału dowodowego Prezes UODO uznał, że Przedsiębiorca nie zweryfikował ASI pod kątem zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych.

9) Ponadto Prezes UODO przyjął, iż Przedsiębiorca dokonał w niewystraczającym zakresie analizy ryzyka wiążącego się z podejmowanymi działaniami zmierzającymi do zapewnienia dostępu do danych osobowych pracownikom pracującym zdalnie.

Przyczyna naruszenia:

Przedsiębiorca nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych oraz nie dokonał weryfikacji ASI pod kątem zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych.

Decyzja PUODO:

1) Kara pieniężna w wysokości 33 012 PLN.

2) Nakaz dostosowania operacji przetwarzania danych osobowych poprzez zaprzestanie powierzenia przetwarzania danych osobowych w oparciu o umowę, która nie zawiera wszystkich niezbędnych elementów wskazanych w RODO.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.50.2021

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) Przeprowadzaj testy nastawione na weryfikację zabezpieczeń programów i aplikacji.

4) Wykonaj analizę ryzyka przed podjęciem działań zmierzających do wprowadzenia zmian w systemie informatycznym.

5) Zawieraj pisemne umowy powierzenia przetwarzania danych osobowych z podmiotami, które uczestniczą w procesie przetwarzania danych osobowych.

6) Dokonuj weryfikacji podmiotu przetwarzającego w kontekście zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych. Czynnikami, które wpływają na określenie wystarczających gwarancji są: wiedza fachowa, wiarygodność, zasoby, reputacja, przestrzeganie zatwierdzonego kodeksu postępowania, certyfikacja.

7) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych, notyfikacji naruszeń ochrony danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska