

Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych



Data wydania decyzji

19 stycznia 2022 r.

Podmiot kontrolowany

PIKA Sp. z o.o.

Wysokość kary

250 135 PLN**FÖRSÄFE**
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 32 ust. 1 i 2 RODO.

Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.



Przedmiot decyzji

Źródło postępowania:

W kwietniu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Fortum Marketing and Sales Polska S.A. (Fortum) polegające na skopiowaniu danych klientów przez nieuprawnione podmioty z programu, którego dostawcą była PIKA Sp. z o.o. (PIKA).

Opis wydarzeń:

1) PIKA została poinformowana przez Fortum o naruszeniu ochrony danych, tj. o fakcie nieuprawnionego skopiowania bazy danych klientów Fortum.

2) Źródłem naruszenia było zlecenie przez Fortum firmie PIKA wprowadzenia zmian w środowisku teleinformatycznym do obsługi archiwum cyfrowego w celu zwiększenia wydajności działania repozytorium.

3) Zmiana polegała na utworzeniu i skonfigurowaniu nowego wirtualnego serwera dla bazy danych klientów Fortum.

4) W związku z powyższym Prezes UODO zwrócił się do PIKA o ustosunkowanie się do treści zgłoszonego przez Fortum naruszenia oraz złożenie wyjaśnień w przedmiotowej sprawie.

5) PIKA w odpowiedzi na otrzymane pismo wyjaśniła, iż w dniu wystąpienia naruszenia prace wykonywane przez PIKA nie były w pełni zakończone, gdyż trwał proces testów oraz zasilania nowoutworzonej bazy danymi.

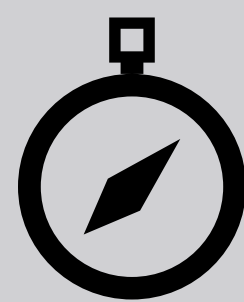
6) Jednocześnie PIKA wskazała, że do wycieku danych doszło w wyniku błędu jednego pracownika, który konfigurując nowy serwer nie podjął czynności, które zapewniałyby bezpieczny kanał komunikacji pomiędzy serwerami środowiska Fortum.

Przyczyna naruszenia:

PIKA na etapie prac rozwojowych nie przetestowała funkcji bezpieczeństwa systemu informatycznego, w którym znajdowały się rzeczywiste dane osobowe.

Decyzja PUODO:

1) Kara pieniężna w wysokości 250 135 PLN.



Kompas FÖRSÄFE

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) Realizując prace rozwojowe w systemach informatycznych, unikaj stosowania danych zawierających dane identyfikujące osobę lub inne poufne dane w charakterze danych testowych.

4) Jeśli do celów testowych w pracach rozwojowych w systemach informatycznych wykorzystujesz dane rzeczywiste, stosuj takie same procedury kontroli dostępu, jak te stosowane w systemach produkcyjnych.

