Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Bułgaria**
Data Protection Commision of Bulgaria (KZLD)

Data wydania decyzji — **28.08.2019 r.**

Podmiot kontrolowany — **National Revenue Agency**

Wysokość kary — **2 600 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 32 (2) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Bułgarski organ nadzorczy w związku z atakiem hakerskim dokonał czynności kontrolnych w Krajowym Urzędzie Skarbowym.

Opis wydarzeń:

1) W wyniku kontroli stwierdzono, że informacje pozyskane podczas ataku hakerskiego, które nielegalnie były rozpowszechniane w Internecie, zawierały dane osobowe łącznie 6 074 140 osób, w tym 4 104 786 żyjących osób, zarówno obywateli bułgarskich, jak i obcokrajowców oraz 1 959 598 osób zmarłych.

2) Dane, jakie zostały publicznie ujawnione obejmowały: nazwiska, osobiste numery identyfikacyjne i adresy obywateli Bułgarii, telefony, adresy e-mail i inne dane kontaktowe, dane z rocznych zeznań podatkowych, dane dotyczące podatku dochodowego od osób fizycznych w rachunku zysków i strat, dane z oświadczeń ubezpieczeniowych, dane o składkach na ubezpieczenie zdrowotne, dane o wydanych aktach z tytułu wykroczeń administracyjnych, dane o dokonanych wpłatach podatku i zobowiązaniach z tytułu ubezpieczenia społecznego, a także dane dotyczące żądanego i zwróconego podatku VAT, który został zapłacony za granicą.

Przyczyna naruszenia:

Atak hakerski skutkujący wyciekiem danych do Internetu.

Decyzja Data Protection Commision of Bulgaria (KZLD):

1) Kara pieniężna w wysokości 5 100 000 BGN (2 600 000 euro).

2) Wdrożenie środków mających na celu poprawę ochrony przetwarzania danych osobowych w aplikacjach związanych ze świadczeniem usług elektronicznych dla obywateli.

3) Przeprowadzanie analizy ryzyka systemów i operacji przetwarzania, w tym ustalonych zasad i obowiązków funkcjonalnych dotyczących przetwarzania każdego systemu informatycznego.

4) Przeprowadzanie oceny skutków w przypadku stwierdzenia „wysokiego ryzyka" dla każdego systemu oraz podjętych środków.

5) Przeprowadzenie oceny wpływu przy pierwszym uruchomieniu nowych systemów informatycznych i aplikacji.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

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

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) Wykonaj wdrożenie procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego.

4) Wykonuj regularne testowanie, mierzenie i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

5) Wykonuj testy podatności systemów informatycznych i aplikacji.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak