KARY ZAGRANICZNYCH URZĘDÓW OCHRONY DANYCH OSOBOWYCH:

FRANCJA

Organ: Commission Nationale de l'Informatique et des Libertés (CNIL)

Podmiot ukarany: SPARTOO SAS (firma sprzedająca obuwie on-line)

Wysokość kary pieniężnej: 250 000 euro

Data wydania decyzji: 28.07.2020 (o karze poinformowano 05.08.2020)

CO SIĘ WYDARZYŁO?

Spartoo prowadzi sprzedaż internetową w trzynastu krajach UE. W maju 2018 r.. organ nadzorczy (CNIL) przeprowadził kontrolę w tej spółce i dopatrzył się nieprawidłowości w przetwarzaniu danych osobowych, a w 2019 r. CNIL zdecydował o wszczęciu postępowania przeciw Spartoo.

Ze względu na to, że spółka przetwarzała dane osobowe osób z innych państw UE, CNIL współpracował ściśle z innymi europejskimi organami ochrony danych. **Jest to pierwsza kara nałożona przez CNIL jako wynik takiej współpracy.**
W decyzji podkreślono, że spółka dopuściła się szeregu naruszeń: niedochowania zasady minimalizacji i ograniczenia czasowego przetwarzania danych, a także braki w spełnieniu obowiązku informacyjnego i zabezpieczeniu danych.

DLACZEGO NAŁOŻONO KARĘ?

Duży wpływ na nałożenie kary miała liczba osób, których dane były przechowywane po upływie niezbędnego okresu ich przetwarzania (**ponad 3 mln klientów i ponad 25 mln potencjalnych klientów**), a także **nagrywanie rozmów telefonicznych** z klientami oraz **przechowywanie danych dotyczących konta bankowego** podawanych przez klientów. Wskazano, że niektóre naruszenia dotyczą **obowiązków istniejących również przed wejściem w życie RODO** (co daje nam wskazówkę do tego, jak organy patrzą na świadomość kontrolowanych firm).

Organ nadzorczy stwierdził następujące naruszenia:

- **naruszenie zasady minimalizacji danych:** nagrywanie w celach szkoleniowych wszystkich rozmów telefonicznych odbieranych przez obsługę klienta (podczas gdy odsłuchuje się tylko jedno nagranie w tygodniu dotyczące danego pracownika). Podczas nagrań utrwalano dane kont bankowych podawane przez klientów, co też jest zbędne dla celów szkoleniowych. Dodatkowo we Włoszech zbierano w celu przeciwdziałania oszustwom kopię "karty zdrowia", która zawiera nawet więcej danych, niż dowód tożsamości (kopia dowodu również była pozyskiwana), a tak zbierany zakres uznano za nadmiarowy.
- **naruszenie zasady ograniczenia czasowego:** np. spółka przechowywała dane ponad 3 mln klientów, którzy nie logowali się do e-sklepu przez ponad 5 lat. W przypadku potencjalnych klientów spółka założyła, że przechowuje dane przez 5 lat od czasu ostatniej aktywności klienta, jednak w praktyce już po 2 latach od ostatniego kontaktu nie korzysta z danych. Ponadto, e-maile i hasła klientów nawet po upływie 5 lat (założony okres retencji) były zachowywane w formie spseudonimizowanej (a nie zanonimizowanej), co pozwala na "odtworzenie" danych.
- **naruszenie spełnienia obowiązku informacyjnego:** np. informowanie klientów, że podstawą prawną przetwarzania ich danych jest zgoda, gdy spółka ma faktycznie inne podstawy, a także niedoinformowanie pracowników o przetwarzaniu danych związanych z nagrywaniem rozmów.
- **naruszenie obowiązku zabezpieczenia danych:** spółka nie stosowała "silnych" haseł do kont klientów. Dodatkowo wg organu przechowywanie skanów karty płatniczej (zbierane w celach przeciwdziałania oszustwom) przez 6 miesięcy w formie niezaszyfrowanej nie jest bezpieczne.

WNIOSKI DLA ADMINISTRATORÓW DANYCH OSOBOWYCH

- ustalenie i przestrzeganie okresów retencji, zwłaszcza biorąc pod uwagę brak aktywności klienta lub potencjalnego klienta
- weryfikacja, czy dane, jakie są zbierane, a zwłaszcza utrwalane "przy okazji" (nagrania, skany, kopie, itp.) są minimalne
- przejrzyste i jasne informowanie o wszystkich celach przetwarzania
- "mocne" hasła, szyfrowanie danych poufnych (jak dotyczących płatności)

Opracowała: Katarzyna Ułasiuk