Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Włochy
Italian Data Protection Authority (Garante)

Data wydania decyzji
22 lipiec 2021 r.

Podmiot kontrolowany
Atac S.p. A.

Wysokość kary
400 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 RODO, Art. 6 RODO, Art. 30 RODO, Art. 32 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy przeprowadził czynności kontrolne w Roma Capitale. Odnosiły się one do oceny funkcjonalności parkometrów i konieczności podawania numeru rejestracyjnego samochodu, za który wnoszona jest opłata. Po ich wykonaniu, włoski organ nadzorczy zadecydował o przeprowadzeniu kontroli w Atac S.p.A (Atac)- spółce odpowiedzialnej za zarządzanie parkometrami.

Opis wydarzeń:

1) W trakcie czynności kontrolnych włoski organ nadzorczy ustalił, iż:

a) Roma Capitale zleciła Atac modernizację parkometrów,

b) po aktualizacji systemu do obsługi parkometrów zaczęto gromadzić dane dotyczące płatności za parking w zakresie: godzina, data rozpoczęcia i zakończenia parkowania, zapłacona kwota oraz numer rejestracyjny pojazdu,

c) w systemie do obsługi parkometrów znajdowało się łącznie 8 600 000 rekordów.

2) Na podstawie zebranego materiału dowodowego, włoski organ nadzorczy dopatrzył się następujących naruszeń:

a) Roma Capitale nie podpisało umowy powierzenia z Atac,

b) Atac nie prowadziła rejestru czynności przetwarzania oraz rejestru wszystkich kategorii czynności przetwarzania,

c) Atac nie określiła okresów retencji przetwarzanych danych osobowych,

d) Atac nie zastosowała środków organizacyjnych i technicznych adekwatnych do zagwarantowania poziomu bezpieczeństwa odpowiedniego do zagrożeń związanych z przetwarzaniem, gdyż:

- przepływy danych do i z systemu nie korzystały z bezpiecznych kanałów komunikacji,
- hasła używane do uwierzytelniania urządzeń pomocniczych były przechowywane w bazie danych w postaci zwykłego tekstu i składały się z 5 znaków,
- nie wdrożono mechanizmu umożliwiającego śledzenie operacji wykonywanych przez użytkowników systemu na danych osobowych,
- użytkownicy systemu do obsługi parkometrów mieli możliwość sprawdzania po numerze rejestracyjnym pojazdu np. zwyczajów danej osoby lub lokalizacji parkingu.

3) Na dzień wydania decyzji część naruszeń została skorygowana.

Przyczyna naruszenia:

Atac nie dopełniła obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja:

1) Kara pieniężna w wysokości 400 000 EUR.

2) Wdrożenie rejestrowania logów systemowych pracy poszczególnych użytkowników oraz wykrywania zachowań anomalnych – w terminie 30 dni od dnia otrzymania decyzji.

3) Wdrożenie środków bezpieczeństwa w celu ochrony przechowywanych informacji zgodnie z wybranymi, maksymalnymi czasami przechowywania – w terminie 30 dni od dnia otrzymania decyzji.

4) Powiadomienie organu nadzorczego o podjętych działaniach wynikających z wydanej decyzji – w terminie 30 dni od dnia otrzymania decyzji.

Źródło:

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9698597

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) Nadając uprawnienia dostępu do danych osobowych w systemie informatycznym pamiętaj, aby były one skorelowane z zakresem obowiązków przypisanym do danego stanowiska.

3) Zawieraj umowy powierzenia przetwarzania danych osobowych z podmiotami, wobec których realizujesz czynności związane z przetwarzaniem danych osobowych.

4) Prowadź rejestru czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 1 RODO.

5) Jeśli występujesz w roli podmiotu przetwarzającego, prowadź rejestr wszystkich kategorii czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 2 RODO.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak