

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)



Data wydania decyzji

22 lipca 2021 r.



Podmiot kontrolowany

Roma Capitale



Wysokość kary

800 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO



Rodzaj naruszenia

Naruszenie art. 5, art. 12, art. 13, art. 25, art. 28, art. 32 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.



Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy otrzymał skargę na Roma Capitale odnoszącą się do funkcjonalności parkometrów, które zostały zainstalowane w 2018 r. a mianowicie do konieczności podawania numeru rejestracyjnego samochodu, za który wnoszona jest opłata.

Opis wydarzeń:

1) Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Roma Capitale celem rozpatrzenia przedmiotowej sprawy.

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

a) w procesie przetwarzania danych osobowych osób uiszczających opłatę uczestniczyła firma Atac s.p.a. oraz Flowbird Italia s.r.l.,

b) system do obsługi parkometrów gromadził dane dotyczące płatności za parking w zakresie: godzina, data rozpoczęcia i zakończenia parkowania, zapłacona kwota oraz numer rejestracyjny pojazdu,

c) od czerwca 2018 r. do listopada 2019 r. w system do obsługi parkometrów znajdowało się łącznie 8 600 000 rekordów.

3) Na podstawie zebranego materiału dowodowego włoski organ nadzorczy dopatrył się następujących naruszeń:

a) Roma Capitale nie realizowało obowiązku informacyjnego wobec osób dokonujących opłaty,

b) Roma Capitale nie podpisało umowy powierzenia z firmą Atac s.p.a. oraz Flowbird Italia s.r.l.,

c) okres retencji przetwarzanych danych osobowych nie został określony,

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

- przepływy danych do i z systemu ATAC 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.

4) Na dzień wydania decyzji część naruszeń została skorygowana.

Przyczyna naruszenia:

Administrator nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

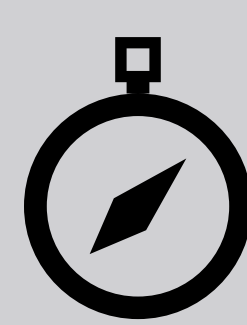
Decyzja Italian Data Protection Authority (Garante):

1) Kara pieniężna w wysokości 800 000 EU.

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.



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, które uczestniczą w procesie przetwarzania danych osobowych.

4) Dokonaj wdrożenia procedur określających zasady pracy na danych osobowych przez podmioty zewnętrzne działające w imieniu Administratora.

5) Realizuj obowiązek informacyjny w sposób przejrzysty oraz zgodnie z wytycznymi art. 13 RODO.

