Kary organów nadzorczych w Unii Europejskiej

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

Data wydania decyzji — **10.06.2021**

Podmiot kontrolowany — **Foodinho s.r.l.**

Wysokość kary — **2 600 000 EUR**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5 (1) a), c), e) RODO, art. 13 RODO, art. 22 (3) RODO, art. 25 RODO, art. 30 (1) a), b), c), f), g) RODO, art. 32 RODO, art. 35 RODO, art. 37 (7) RODO
Nieprzestrzeganie ogólnych zasad przetwarzania danych

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy dokonał czynności kontrolnych w Foodinho s.r.l. (Spółka).

Opis wydarzeń:

1) Przedmiotem kontroli było przetwarzanie danych osobowych kierowców, dostarczających zamówione jedzenie.

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

a) naruszenie prawa dostępu do informacji – Spółka nie przekazywała kierowcom wszystkich informacji o przetwarzaniu ich danych osobowych, jakie zgodnie z RODO powinny być podane,

b) naruszenie zasady minimalizacji przetwarzania danych osobowych – Spółka przetwarzała dane osobowe kierowców w szerszym celu niż powinna,

c) naruszenie zasady ograniczenia czasowego – Spółka przechowywała dane osobowe kierowców dłużej niż było to konieczne,

d) naruszenie prawa do informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu – Spółka nie informowała kierowców o zautomatyzowanym podejmowaniu decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania danych,

e) niepodanie danych kontaktowych do Inspektora Ochrony Danych, który był wyznaczony w ramach grupy kapitałowej,

f) nieprawidłowości dotyczące algorytmów systemów informatycznych – Spółka nie informowała kierowców o działaniu systemu oraz nie gwarantowała dokładności i poprawności wyników algorytmów, wykorzystywanych do ich oceny,

g) brak przeprowadzenia oceny skutków dla ochrony danych dotyczących geolokalizacji i aplikacji profilujących kierowców,

h) brak uwzględnienia ochrony danych osobowych w fazie projektowania – Spółka nie dokonała właściwej konfiguracji systemów informatycznych w szczególności w zakresie dostępu do danych osobowych,

i) błędy w prowadzonym rejestrze czynności przetwarzania danych osobowych – Spółka nie uwzględniła w rejestrze wszystkich informacji, jakie zgodnie z RODO powinny się w nim znaleźć; zdaniem włoskiego organu nadzorczego brakowało również informacji o dacie sporządzenia rejestru oraz dacie jego ostatniej aktualizacji.

3) Naruszenie ochrony danych osobowych dotyczyło łącznie około 18 684 kierowców.

Przyczyna naruszenia:

Administrator nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja Italian Data Protection Authority (Garante):

1) Kara pieniężna w wysokości 2 600 000 EUR.

2) Zobowiązanie Spółki do:
a) prawidłowego sporządzenia dokumentów, takich jak: obowiązek informacyjny, rejestr czynności przetwarzania danych osobowych, ocena skutków dla ochrony danych – w terminie 60 dni od dnia otrzymania niniejszej decyzji,
b) określenia okresów retencji przetwarzanych danych osobowych – w terminie 60 dni od dnia otrzymania niniejszej decyzji,
c) określenie adekwatnych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, w odniesieniu do zautomatyzowanego przetwarzania, w tym profilowania dokonywanego za pośrednictwem systemu informatycznego – w terminie 60 dni od dnia otrzymania niniejszej decyzji,
d) określenie adekwatnych środków mających na celu okresową weryfikację poprawności i dokładności wyników systemów algorytmicznych, aby zminimalizować ryzyko błędów a tym samym dyskryminacji, np. w sferze ocen i punktacji kierowców – w terminie 60 dni od dnia otrzymania niniejszej decyzji,
e) zastosowania się do zasady minimalizacji przetwarzania danych osobowych – w terminie 60 dni od dnia otrzymania niniejszej decyzji.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

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

2) Opracuj rejestr czynności przetwarzania danych osobowych zgodnie z wytycznymi art. 30 ust. 1 RODO.

3) Weryfikuj procesy przetwarzania danych osobowych pod kątem zasady minimalizacji i legalności przetwarzania danych osobowych a także w aspekcie czasu ich przetwarzania.

4) Pozyskuj zgody na przetwarzanie danych w celu profilowania oraz wyjaśnij na czym będzie polegało profilowanie oraz czym ono skutkuje dla danej osoby.

5) Wykonaj ocenę skutków dla ochrony danych, gdy:

a) przetwarzanie danych osobowych z dużym prawdopodobieństwem może powodować wysokie naruszenie praw lub wolności osób fizycznych,

b) przetwarzanie danych osobowych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu,

c) dane osobowe szczególnej kategorii oraz dane dotyczące wyroków sądowych i czynów zabronionych są przetwarzane na dużą skalę,

d) operacje przetwarzania danych osobowych zawarte są w wykazie upublicznionym przez organ nadzorczy.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak