Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

20 październik 2022 r.

Podmiot kontrolowany

Douglas Italia S.p.a.

Wysokość kary

1 400 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) b), e) RODO, Art. 5 (2) RODO, Art. 6 RODO, Art. 7 RODO, Art. 12 (1) RODO, Art. 13 (2) a) RODO, Art. 24 RODO, Art. 25 (1) RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy otrzymał skargę na Douglas Italia S.p.a. (Douglas) odnoszącą się do braku odpowiedzi na wniosek o realizację praw podmiotów danych.

Opis wydarzeń:

1) Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Douglas celem rozpatrzenia przedmiotowej sprawy, a w szczególności weryfikacji sposobu realizacji praw podmiotów danych oraz wykorzystania danych osobowych w celach marketingowych i profilowania.

2) W trakcie czynności kontrolnych włoski organ nadzorczy ustalił, iż Douglas powstał z połączenia 3 spółek i w związku z tym w CRM posiada dane osobowe około 10 milionów klientów.

3) Na podstawie zebranego materiału dowodowego włoski organ nadzorczy dopatrzył się naruszenia:

a) zasady legalności przetwarzania i warunków wyrażania zgody – klient rejestrując się w aplikacji Douglas wyraża jedną zgodę na różne cele, w tym marketing Douglas, marketing firm partnerskich Douglas i profilowanie,

b) zasady ograniczenia celu i zasady ograniczenia przechowywania – Douglas przechowuje w CRM dane osobowe klientów 3 spółek, którzy nie zdecydowali się na wyrobienie nowej karty lojalnościowej pod marką Douglas,

c) zasady rozliczalności i obowiązku wdrożenia adekwatnych środków technicznych i organizacyjnych – Douglas nie był w stanie wykazać czy 3 spółki zrealizowały wobec klientów obowiązek informacyjny oraz odebrały zgodę na przetwarzanie danych osobowych,

d) zasady przejrzystości – Douglas w obowiązku informacyjnym spełnianym wobec klientów wskazuje okresy retencji danych osobowych, które w praktyce nie są realizowane,

e) zasady rozliczalności, obowiązku wdrożenia adekwatnych środków technicznych i organizacyjnych oraz obowiązku uwzględnienia ochrony danych w fazie projektowania – Douglas wykorzystywał numery telefonów klientów do telemarketingu i marketingu poprzez SMS niezależnie od tego, na którą formę komunikacji klient wyraził zgodę,

f) zasady rozliczalności, obowiązku wdrożenia adekwatnych środków technicznych i organizacyjnych oraz zasady przejrzystości – Douglas nie był w stanie wyjaśnić w jakim celu i jak długo przechowuje dane osobowe osób pozostawiających komentarz pod artykułami na blogu.

Przyczyna naruszenia:

Douglas nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja:

1) Kara pieniężna w wysokości 1 400 000 EUR.

2) Nakaz modyfikacji ustawień aplikacji Douglas gwarantujących rozróżnienie na: informacje dotyczące prywatności, informacje o plikach cookies, informacje o warunkach sprzedaży i informacje o danych osobowych.

3) Nakaz usunięcia danych osobowych klientów 3 spółek pochodzących z okresu dłuższego niż 10 lat z wyjątkiem danych klientów, wobec których toczy się postępowanie sądowe lub pozasądowe – w terminie 15 dni od otrzymania decyzji.

4) Nakaz usunięcia lub pseudonimizacji danych osobowych klientów 3 spółek pochodzących z okresu krótszego niż 10 lat – w terminie 30 dni od otrzymania decyzji.

5) Jeśli Douglas zdecyduje się na pseudonimizację danych, nakazuje się poinformowanie klientów o planowanych działaniach dając im możliwość odnowienia karty lojalnościowej przez 6 miesięcy od dnia publikacji komunikatu.

6) Nakaz usunięcia danych osobowych klientów, którzy nie skorzystali z powyższej możliwości odnowienia karty lojalnościowej – w terminie 15 dni od upłynięcia wspomnianego 6-miesięcznego terminu.

7) Nakaz przyjęcia odpowiednich zabezpieczeń technicznych i organizacyjnych zapewniających, że przechowywanie danych osobowych klientów odbywa się z poszanowaniem zasady ograniczenia celu i minimalizacji danych.

Źródło:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9825667

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Zaprojektuj mechanizm pozyskiwania zgody na przetwarzanie danych osobowych. Pamiętaj, że zgoda na przetwarzanie danych osobowych musi być świadoma i dobrowolna. Dlatego nie stosuj odgórnie zaznaczonych pól oraz nie traktuj braku działania ze strony osoby, których dane dotyczą, jako zgody.

2) Zgodę na przetwarzanie danych sformułuj w sposób jednoznaczny, tzn. użytkownik musi być świadomy na co i w jakim zakresie wyraża zgodę.

3) Zgodę na przetwarzanie danych sformułuj w sposób konkretny, tzn. użytkownik musi być świadomy w jakim celu wyraża zgodę.

4) Zweryfikuj zgody na przetwarzanie danych osobowych pod kątem celu przetwarzania (jeden cel przetwarzania = jedna zgoda) oraz dobrowolności wyrażenia zgody.

5) Realizuj obowiązek informacyjny w sposób przejrzysty oraz zgodnie z wytycznymi art. 13 i 14 RODO.

6) Opracuj i wdróż procedurę retencji danych oraz regularnie weryfikuj procesy przetwarzania danych osobowych w aspekcie czasu przetwarzania danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska