Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

28 lutego 2023 r.

Podmiot kontrolowany

Ediscom S.p.a.

Wysokość kary

300 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) a), b), c) RODO, Art. 6 RODO, Art. 7 RODO, Art. 14 RODO, Art. 25 RODO
Nieprzestrzeganie ogólnych zasad przetwarzania danych .

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy dokonał czynności kontrolnych w Ediscom S.p.a. (Ediscom).

Opis wydarzeń:

1. Przedmiotem kontroli była weryfikacja baz danych wykorzystywanych do celów marketingowych, kryteria wyboru dostawców oraz możliwość odpowiadania na żądania osób, których dane dotyczą.

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

a) świadczy usługi marketingowe dla średnich i dużych przedsiębiorstw polegające na wysyłaniu smsów i e-maili,

b) świadczy również usługi dostępu do własnych baz danych na potrzeby telemarketingowe swoich klientów,

c) posiada w swojej bazie danych ok. 21 milionów rekordów,

d) pozyskuje dane do bazy danych z własnych portali, od zewnętrznych dostawców, od firm dających dostęp do własnych baz danych

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

a) zasady minimalizacji – w formularzach zbierano więcej danych niż było to niezbędne do realizacji celu przetwarzania,

b) dobrowolności wyrażenia zgody – Ediscom nakłaniał użytkowników do wyrażenia zgody na przetwarzanie ich danych w celach marketingowych oraz na ich przekazanie podmiotom trzecim,

c) dobrowolności wyrażenia zgody – Ediscom zakładał automatycznie konta użytkownikom na stronach internetowych, na które użytkownik był przekierowywany po kliknięciu w link, który się im wyświetlał,

d) zasady przejrzystości – niektóre strony internetowe nie miały umieszczonej w ogólnie dostępnym miejscu polityki prywatności a tym samym nie było informacji o administratorze danych,

e) zasady legalności – Ediscom zbierał od użytkowników dane o osobach trzecich bez pozyskania ich zgody na przetwarzanie danych osobowych,

f) prawidłowego określenia ról – Ediscom został błędnie określony jako administrator danych dla baz danych, do których miał jedynie dostęp i nie był ich właścicielem.

Przyczyna naruszenia:

Ediscom pozyskiwał dane osobowe do swoich baz danych bez respektowania zasad ochrony danych osobowych.

Decyzja:

1. Kara pieniężna w wysokości 300 000 EUR.

2. Zakaz przetwarzania danych osobowych, w szczególności danych przekazanych przez innych użytkowników, bez odpowiedniej podstawy prawnej.

3. Zakaz przetwarzania danych osobowych zebranych w ramach interakcji różnych usług, gdy nie jest możliwe udokumentowanie zgody wyrażonej dobrowolnie przez zainteresowaną stronę.

Źródło:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870014

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. Zweryfikuj bazy marketingowe w zakresie posiadania udokumentowanej zgody na działania marketingowe oraz realizuj działania marketingowe jedynie wobec osób, które wyraziły na to zgodę.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska