

## Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

**Włochy**

Italian Data Protection Authority (Garante)



Data wydania decyzji

**25 listopad 2021 r.**



Podmiot kontrolowany

**B&T S.p.A.**



Wysokość kary

**400 000 EUR**

FORSAFE  
BEZPIECZENSTWO PONAD WSZYSTKO



### Rodzaj naruszenia

Art. 5 (1) a) RODO, Art. 6 (1) a) RODO, Art. 12 RODO, Art. 13 RODO, Art. 14 RODO, Art. 21 RODO  
Niewystarczająca podstawa prawna do przetwarzania danych.



### Przedmiot decyzji

#### Źródło postępowania:

Włoski organ nadzorczy otrzymał skargi na B&T S.p.A. (B&T) odnoszące się do otrzymywania niezamówionych wiadomości tekstowych, których celem były działania marketingowe.

#### Opis wydarzeń:

**1)** Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w B&T celem rozpatrzenia przedmiotowej sprawy.

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

**a)** B&T zlecił realizację działań marketingowych firmie Aimon,

**b)** Aimon dokonał wysyłki wiadomości tekstowych do bazy osób pozyskanej od innych podmiotów bez skontrolowania legalności pozyskania danych osobowych przez te podmioty,

**c)** Aimon wysyłał również wiadomości tekstowe do osób, które wyraziły sprzeciw przeciwko przetwarzaniu ich danych osobowych.

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

**a)** brak określenia ról i obowiązków – odbiorcy wiadomości tekstowych nie wiedzieli kto jest administratorem ich danych osobowych oraz do kogo mogą zwrócić się z wnioskami o realizację ich praw,

**b)** brak realizacji zasady rozliczalności – B&T nie był w stanie udowodnić, że podmioty z nim współpracujące dysponowały podstawą legalizującą przetwarzanie danych osobowych potencjalnych klientów,

**c)** brak realizacji prawa do sprzeciwu – Aimon realizował działania marketingowe pomimo sprzeciwu wobec przetwarzania danych osobowych w tym celu,

**d)** brak realizacji zasady przejrzystości – B&T nie był w stanie zapewnić odbiorcom wiadomości tekstowych realizacji ich praw, gdyż nie dysponował informacjami o nich,

**e)** brak realizacji przejrzystego obowiązku informacyjnego – odbiorcy wiadomości tekstowych nie wiedzieli kto jest administratorem ich danych osobowych.

**4)** Naruszenie ochrony danych osobowych trwało od 2018 r. do 2020 r. W tym czasie wysłano 2 490 000 wiadomości tekstowych w 2018 r., 1 800 000 wiadomości tekstowych w 2019 r. oraz 3 220 000 wiadomości tekstowych w 2020 r.

**5)** B&T w związku z zaistniałą sytuacją zdecydował o rozwiązaniu umowy z Aimon.

#### Przyczyna naruszenia:

Brak kontroli nad realizacją działań marketingowych wykonywanych przez podmioty zewnętrzne.

#### Decyzja:

Kara pieniężna w wysokości 400 000 EUR.

#### Źródło:

<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9737185>



### 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 zgody na działania marketingowe oraz realizuj działania marketingowe jedynie wobec osób, które wyraziły na to zgodę.

**6)** Dokonaj wdrożenia systemów kontroli „łańcucha” zbierania danych osobowych od momentu pierwszego kontaktu potencjalnego klienta.

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

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

**9)** Opracuj i wdróż procedury realizacji praw podmiotów danych.

**10)** Wdróż środki techniczne i organizacyjne dotyczące obsługi wniosków o skorzystanie z praw podmiotów danych.

