

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Hiszpania

Spanish Data Protection Authority (AEPD)



Data wydania decyzji

04 luty 2022 r.



Podmiot kontrolowany

SEGURCAIXA ADESLAS, S.A. DE SEGUROS Y REASEGUROS



Wysokość kary

600 000 EUR

FORSAFE
BEZPIECZENSTWO PONAD WSZYSTKO



Rodzaj naruszenia

Art. 6 RODO, Art. 17 RODO, Art. 28 RODO.
Niewystarczająca podstawa prawna do przetwarzania danych.



Przedmiot decyzji

Źródło postępowania:

Hiszpański organ nadzorczy otrzymał skargę na SEGURCAIXA ADESLAS, S.A. DE SEGUROS Y REASEGUROS (SEGURCAIXA ADESLAS) odnoszącą się do braku uwzględnienia prawa do usunięcia danych osobowych.

Opis wydarzeń:

1) Hiszpański organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w SEGURCAIXA ADESLAS celem rozpatrzenia przedmiotowej sprawy.

2) W trakcie czynności kontrolnych włoski organ nadzorczy ustalił, iż SEGURCAIXA ADESLAS zajmuje się sprzedażą polis ubezpieczeniowych i współpracuje w tym zakresie z zewnętrznymi agentami ubezpieczeniowymi.

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

a) brak realizacji zasady legalności przetwarzania danych osobowych – SEGURCAIXA ADESLAS nie dysponował podstawą legalizującą przetwarzanie danych osobowych i wysyłał wiadomości marketingowe do Skarżącego pomimo, iż znajdował się on na Liście Robinsona,

b) brak realizacji prawa do usunięcia danych osobowych – SEGURCAIXA ADESLAS nie odpowiadał na wnioski Skarżącego.

Przyczyna naruszenia:

Brak kontroli nad realizacją działań marketingowych.

Decyzja:

Kara pieniężna w wysokości 300 000 EUR.

Źródło:

<https://www.aepd.es/es/documento/ps-00322-2021.pdf>



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) Opracuj i wdróż procedury realizacji praw podmiotów danych.

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

