Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Hiszpania**
Spanish Data Protection Authority (AEPD)

Data wydania decyzji — **13.01.2021 r.**

Podmiot kontrolowany — **CaixaBank S.A.**

Wysokość kary — **6 000 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 6, Art. 13 i Art. 14 RODO
Niewystarczająca podstawa prawna do przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

W styczniu 2018 r. do Hiszpańskiego Urzędu Ochrony Danych Osobowych wpłynęła skarga od osoby prywatnej zaś marcu 2019 r. wpłynęło pismo od Stowarzyszenia Konsumentów i Użytkowników na CaixaBank SA.

Opis wydarzeń:

1) Przedmiotem skargi było nałożenie na klientów banku obowiązku zaakceptowania nowych warunków ochrony danych osobowych, w szczególności odnoszących się do przekazywania danych osobowych do wszystkich spółek z Grupy CaixaBank.

2) Skarżący nie miał jednocześnie możliwości niewyrażenia zgody na przekazywanie danych osobowych do wszystkich spółek, a w celu jej odwołania musiał wysłać pisma w tej sprawie do każdej ze spółek z Grupy CaixaBank osobno.

3)W odpowiedzi na pismo Hiszpańskiego Urzędu Ochrony Danych Osobowych CaixaBank wyjaśnił, że podstawą jego działań było dostosowanie zapisów do wymogów RODO oraz usprawnienie wymiany danych w Grupie CaixaBank. W związku z powyższym Spółka postanowiła odbierać zgody od klientów na przetwarzanie ich danych osobowych m.in. w celach handlowych dla całej Grupy CaixaBank.

4) CaixaBank poinformował dodatkowo, że w Grupie CaixaBank został wdrożony scentralizowany system realizacji praw podmiotów danych, w którym można dokonać odwołania zgody dla całej Grupy CaixaBank.

5) W międzyczasie Stowarzyszenie Konsumentów i Użytkowników złożyło roszczenie przeciwko CaixaBank, którego przedmiotem była obowiązkowa umowa, w ramach której pozyskiwane były dane osobowe oraz zbierane zgody na ich przetwarzanie i przekazywanie do podmiotów w Grupie CaixaBank.

6) Głównym zarzutem Stowarzyszenia Konsumentów i Użytkowników był brak możliwości negocjacji zapisów ww. umowy.

7) AEPD po zebraniu materiału dowodowego stwierdził naruszenie artykułów 13 i 14 RODO uznając, iż:

a) informacje wskazane w różnych dokumentach i kanałach nie są jednolite,

b) w polityce prywatności stosowana jest nieprecyzyjna terminologia,

c) klienci nie są precyzyjnie informowani o kategorii danych osobowych, które będą przetwarzane,

d) klienci nie są informowani o celu przetwarzania oraz jego podstawie prawnej, w szczególności w odniesieniu do przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu,

e) klienci nie są precyzyjnie informowani o profilowaniu, w tym o rodzaju profili, które mają być wykonane oraz ich konkretnych zastosowaniach, do których mają być wykorzystywane,

f) brak jednolitości w przekazywaniu informacji o wykonywaniu praw podmiotów danych, możliwości wniesienia roszczeń do Hiszpańskiego Urzędu Ochrony Danych Osobowych, powołaniu Inspektora Ochrony Danych oraz jego danych kontaktowych, a także informacjach dotyczących okresów przechowywania danych osobowych.

Przyczyna naruszenia:

W toku kontroli AEPD wskazał, że CaixaBank niewystarczająco uzasadnił podstawy prawne przetwarzania danych osobowych, w szczególności w odniesieniu do przetwarzania opartego na prawnie uzasadnionym interesie. Nie respektował także wytycznych odnoszących się do pobierania zgody (biorąc pod uwagę, że zgoda musi być konkretna, jednoznaczna i świadomie wyrażona) i uzyskiwał zgody klientów na przetwarzanie ich danych osobowych a później bezprawnie przekazywał je do spółek z Grupy CaixaBank.

Decyzja AEPD:

1) Kara pieniężna w wysokości 2 000 000 euro za naruszenie art. 13 i 14 RODO,

2) Kara pieniężna w wysokości 4 000 000 euro za naruszenie art. 6 RODO,

3) Dostosowanie w ciągu 6 miesięcy do przepisów o ochronie danych osobowych:

a) operacji przetwarzania osobowych,

b) informacji przekazywanych klientom,

c) procedury opisującej przetwarzanie danych osobowych,

d) zgód na przetwarzanie danych osobowych.

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

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

6) Opracuj politykę prywatności i obowiązek informacyjny, które w sposób jasny i precyzyjny będą informowały osoby, których dane dotyczą, o przetwarzaniu ich danych osobowych. Staraj się używać prostego języka, unikać zdań i skomplikowanych struktur językowych. Istotne jest również to, aby cele i podstawa prawna przetwarzania danych osobowych były łatwe do zrozumienia.

7) Powołując się przy przetwarzaniu danych osobowych na usprawiedliwiony interes administratora, pamiętaj o wykonaniu testu równowagi.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak