Kary organów nadzorczych w Unii Europejskiej

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

Data wydania decyzji — **04.05.2021 r.**

Podmiot kontrolowany — **EDP Energía, S.A.U**

Wysokość kary — **1 500 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 13 RODO, Art. 25 RODO
Niedostateczne wypełnienie obowiązków informacyjnych.

Przedmiot decyzji

Źródło postępowania:

Do hiszpańskiego organu nadzorczego wpłynęła skarga na EDP Energía, S.A.U. (EDP), której przedmiotem było przetwarzanie danych osobowych w umowie o dostawę energii elektrycznej bez zgody Skarżącej.

Opis wydarzeń:

1) Hiszpański organ nadzorczy w trakcie czynności kontrolnych dopatrzył się następujących naruszeń:

a) brak uwzględnienia w analizie ryzyka ryzyk odnoszących się do podpisywania umów z EDP przez przedstawicieli/pełnomocników w imieniu właścicieli nieruchomości,
b) niekompletne informacje zawarte w zgodzie na przetwarzanie danych osobowych,
c) pozyskiwanie jednej zgody na przetwarzanie danych osobowych w dwóch różnych celach,
d) przetwarzanie danych osobowych w celu zautomatyzowanego podejmowania decyzji, w tym profilowania, bez odebrania świadomej zgody oraz poinformowania podmiotu danych o przysługujących mu prawach,
e) złamanie zasady przejrzystości poprzez spełnienie niekompletnego obowiązku informacyjnego oraz brak łatwego odnalezienia obowiązku informacyjnego na stronie www,
f) wskazanie w obowiązku informacyjnym dwóch administratorów bez przypisania każdemu z nich celów przetwarzania danych osobowych.

2) Hiszpański organ nadzorczy uznał również, iż EDP:

a) nie wdrożył środków technicznych i organizacyjnych w celu wyeliminowania ryzyk podczas podpisywania umów z EDP przez przedstawicieli/pełnomocników w imieniu właścicieli nieruchomości,
b) nie wdrożył środków technicznych i organizacyjnych w celu wyeliminowania ryzyk związanych z odbieraniem zgód na przetwarzanie danych osobowych od przedstawicieli/pełnomocników a wyrażanych w imieniu właścicieli nieruchomości.

Przyczyna naruszenia:

Decyzje Administratora, które doprowadziły do naruszenia zasad ochrony danych osobowych.

Decyzja Spanish Data Protection Authority (AEPD):

Kara pieniężna w wysokości 1 500 000 EUR.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Wykonuj cyklicznie udokumentowaną analizę ryzyka uwzględniającą charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

2) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

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

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

5) 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.

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

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

8) Dokonaj wdrożenia środków organizacyjnych lub technicznych umożliwiających udowodnienie otrzymania zgody podmiotu danych, w szczególności w sposób pozwalający na utrwalenie faktu otrzymania zgody.

9) Opracuj obowiązek informacyjny, który w sposób jasny i precyzyjny będzie informował 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.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak