

Kary organów nadzorczych w Unii Europejskiej

**Kraj oraz organ nadzorczy****Włochy**

Italian Data Protection Authority (Garante)

**Data wydania decyzji****24 listopad 2022 r.****Podmiot kontrolowany****Areti S.p.A****Wysokość kary****1 000 000 EUR****Rodzaj naruszenia**

Art. 5 (1) d), e) RODO, Art. 5 (2) RODO, Art. 12 RODO, Art. 15 RODO, Art. 24 RODO
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

**Przedmiot decyzji****Źródło postępowania:**

Włoski organ nadzorczy otrzymał skargę na Areti S.p.A. (Areti) odnoszącą się do braku aktualizacji danych Skarżącej i sklasyfikowania jej jako klienta zalegającego z płatnością, co uniemożliwiło jej zmianę dostawcy energii elektrycznej.

Opis wydarzeń:

1) Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Areti celem rozpatrzenia przedmiotowej sprawy.

2) W trakcie czynności kontrolnych włoski organ nadzorczy ustalił, iż Areti jest dostawcą energii elektrycznej, który w wyniku niezgodności w wewnętrznych systemach posiadał nieaktualne dane w swoich bazach danych.

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

a) zasady rzetelności i prawidłowości – Areti w wyniku błędnego zastosowania zapytania ekstrakcji informacji o zaległościach klientów końcowych posiadało nieaktualne dane w swoich bazach danych,

b) zasady rzetelności – Areti przechowywało w swoich systemach przez krótki czas (kilka godzin) dane o zaległościach klientów końcowych,

c) zasady ograniczenia przechowywania – Areti stosowało jednolity czas retencji danych osobowych klientów niezależnie od rodzajów ich przetwarzania,

d) realizacji praw podmiotów danych – Areti nie udzieliła odpowiedniej odpowiedzi na wnioski o udzielenie dostępu do danych osobowych Skarżącej,

e) zastosowania środków technicznych i organizacyjnych – Areti nie wdrożyło środków adekwatnych do charakteru, kontekstu, celu i ryzyka przetwarzania danych.

4) W związku z powyższym 47 767 klientów miało trudności w zmianie dostawcy energii elektrycznej ze względu na nieaktualne dane.

5) Na dzień wydania decyzji Areti:

a) wdrożyło zmiany w wewnętrznych systemach,

b) zaczęło usuwać dane zgodnie z przyjętą polityką retencji danych,

c) zaplanowało szkolenia.

Przyczyna naruszenia:

Areti nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja:

1) Kara pieniężna w wysokości 1 000 000 EUR.

2) Nakaz wdrożenia zmian w wewnętrznych systemach – w terminie 6 miesięcy od doręczenia niniejszej decyzji.

Źródło:

<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9832979>

**Kompas FORSAFE****JAK UNIKAĆ TAKICH NARUSZEŃ?**

1) 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.

2) Opracuj i wdróż procedurę retencji danych oraz regularnie weryfikuj procesy przetwarzania danych osobowych w aspekcie czasu przetwarzania danych osobowych.

3) Opracuj i wdróż procedury realizacji praw podmiotów danych.

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

