

Kary organów nadzorczych w Unii Europejskiej

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

Italian Data Protection Authority (Garante)

**Data wydania decyzji****1 czerwca 2023 r.****Podmiot kontrolowany****Ew Business Machines S.p.A.****Wysokość kary****20 000 EUR****FORSAFE**
BEZPIECZENSTWO PONAD WSZYSTKO**Rodzaj naruszenia**

Art. 5 (1) a), c), art. 9, art. 13 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

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

Włoski organ nadzorczy otrzymał skargę na Ew Business Machines S.p.A. (Spółka) odnoszącą się do korzystania z monitoringu wizyjnego umożliwiającego nagrywanie obrazu i dźwięku, pobierania od pracowników odcisków palców oraz zbierania informacji o geolokalizacji pracowników.

Opis wydarzeń:

1. Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych celem rozpatrzenia przedmiotowej sprawy oraz zwrócił się do Spółki z prośbą o przedłożenie wyjaśnień.

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

a) Spółka za pomocą monitoringu wizyjnego rejestrowała obraz oraz dźwięk w czasie rzeczywistym,

b) do nagrań z monitoringu wizyjnego miał dostęp właściciel Spółki oraz jego żona i dzieci,

c) Spółka nie zrealizowała obowiązku informacyjnego wobec pracowników oraz innych osób objętych monitoringiem wizyjnym,

d) Spółka pobierała od pracowników odciski palców w celu aktywacji i dezaktywacji systemu alarmowego,

e) Spółka monitorowała personel techniczny za pomocą aplikacji do zbierania informacji o geolokalizacji,

f) Spółka nie zrealizowała obowiązku informacyjnego wobec pracowników w związku ze zbieraniem informacji o geolokalizacji.

3. Na dzień zakończenia kontroli Spółka zmieniła system alarmowy i zaprzestała pobierania od pracowników odcisków palców.

Przyczyna naruszenia:

Spółka nadmiarowo monitorowała swoich pracowników oraz przetwarzała dane biometryczne swoich pracowników bez podstawy prawnej.

Decyzja:

1. Kara pieniężna w wysokości 20 000 EUR.

2. Zakaz przetwarzania dokonywanego z wykorzystaniem monitoringu wizyjnego.

3. Zakaz ciągłego monitorowania położenia pracownika.

Źródło:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9913830>

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

1. Dane biometryczne mogą być wykorzystywane m.in.: w celu

a) zapewnienia bezpieczeństwa osobowego,

b) zapewnienia bezpieczeństwa przemysłowego,

c) ochrony informacji,

d) weryfikacji osób podejrzanych i ocenie ich udziału w przestępstwach,

e) wydawania dokumentów identyfikacyjnych (paszportów),

f) kontroli dostępu do określonych sfer bezpieczeństwa.

2. Wykorzystując dane biometryczne zawsze należy rozważyć, czy jest to adekwatne w stosunku do celu, jaki będzie realizowany.

3. Jeśli w swojej pracy zdecydujesz się na pozyskiwanie danych o geolokalizacji warto zapoznać się z wytycznymi 01/2020 dotyczącymi przetwarzania danych osobowych w kontekście pojazdów podłączonych do Internetu i aplikacji związanych z mobilnością. Zgodnie z nimi należy przestrzegać zasad, na które warto zwrócić uwagę a są nimi:

a) odpowiednia konfiguracja częstotliwości dostępu do danych dotyczących lokalizacji i poziomu ich szczegółowości w stosunku do celu przetwarzania,

b) przekazywanie prawidłowych informacji dotyczących celu przetwarzania oraz realizacja obowiązku informacyjnego,

c) uzyskanie ważnej (dobrowolnej, konkretnej i świadomej) zgody, która jest odrębna w stosunku do ogólnych warunków sprzedaży lub użytkowania – gdy przetwarzanie odbywa się na podstawie udzielonej zgody,

d) uruchamianie usług lokalizacji tylko wtedy, gdy użytkownik włączy funkcjonalność, która wymaga informacji o lokalizacji pojazdu, a nie w sposób domyślny i ciągły po uruchomieniu pojazdu,

e) informowanie użytkownika o tym, że usługi lokalizacji zostały włączone, w szczególności za pomocą ikon,

f) dostępność opcji umożliwiającej wyłączenie usług lokalizacji w dowolnym momencie,

g) określenie ograniczonego czasu przechowywania danych.

