

# COMPLIANCE INSIGHTS

---

Vol. 52

Naruszenia  
RODO kosztują –  
McDonald's  
zapłaci blisko 17  
mln zł kary



# 1. Rekordowa kara dla McDonald's

Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył na McDonald's Polska **karę w wysokości 16,93 mln zł za szereg poważnych naruszeń przepisów RODO.**

Dodatkowo, karą pieniężną w kwocie blisko 184 tys. zł nałożył na firmę 24/7 Communication odpowiedzialną za przetwarzanie danych na zlecenie McDonald's.

Są to kolejne podmioty ukarane za nieprawidłowości związane z brakiem właściwego wyboru i kontroli podmiotów przetwarzających dane.



## 2. Na czym polegało naruszenie?

Prezes UODO wszczął postępowanie w wyniku zgłoszonego przez McDonald's naruszenia ochrony danych osobowych, które polegało na udostępnieniu w publicznym katalogu danych pracowników McDonald's i jego franczyzobiorców, w tym imion i nazwisk, numerów PESEL, numerów paszportów, danych dotyczących świadczonej pracy i jej grafików.

Do naruszenia doszło w wyniku nieprawidłowej konfiguracji serwera, umożliwiającej podgląd do jego katalogów, w tym kopii bazy danych z aplikacji służącej do zarządzania grafikami pracowniczymi zawierającej dane osobowe.



### 3. Nieprawidłowości w zarządzaniu danymi

---

McDonald's zlecił zarządzanie grafikami pracy pracowników własnych i franczyzobiorców firmie zewnętrznej, nie analizując jednak ryzyka ani nie wdrażając odpowiednich zabezpieczeń danych.

Administrator, mimo takich możliwości technicznych, nie miał własnego dostępu do systemu, którym zarządzał wyłącznie podmiot przetwarzający. Z uwagi na brak uprawnień do zarządzania zasobami i konfiguracją modułu grafików pracowniczych, realnie nie posiadał możliwości kontroli systemu, w którym przetwarzane były jego dane.



## 4. Czy umowa powierzenia wystarczy?

Choć pomiędzy McDonald's i 24/7 Communication zawarta została umowa powierzenia danych, jej postanowienia nie były w praktyce realizowane, w szczególności w zakresie prawa administratora do prowadzenia audytów i inspekcji.

**Administrator nie nadzorował należycie przetwarzania danych przez zaangażowanego procesora, co w konsekwencji było przyczyną zaistniałego incydentu.**



# 5. Ocena Prezesa UODO

**Prezes UODO podkreślił, że ochrona danych osobowych to proces ciągły, wymagający współpracy administratora i podmiotu przetwarzającego.**

W tym przypadku zabrakło podstawowych działań prewencyjnych, analizy ryzyka oraz wdrożenia odpowiednich środków technicznych i organizacyjnych bezpieczeństwa danych, w szczególności w zakresie regularnego testowania, mierzenia i oceniania systemu informatycznego wykorzystywanego do przetwarzania danych.



## 6. Odpowiedzialność obu stron

---

Prezes UODO przypomniał, że zarówno administrator, jak i podmiot przetwarzający ponoszą odpowiedzialność za ochronę danych. Na administratorze ciąży obowiązek weryfikacji potencjalnego podmiotu przetwarzającego, w tym czy daje on gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa podmiotów danych. Sam powinien także ocenić cały proces przetwarzania m.in. pod kątem zasady minimalizacji danych.



## **6. Odpowiedzialność obu stron**

---

**Na procesorze ciąży zaś m.in. obowiązek wyboru właściwego subprocesora, któremu podzleca czynności przetwarzania oraz zawarcia z nim umowy podpowierzenia, która będzie na taki podmiot nakładać obowiązki analogiczne, jak administrator nałożył na samego procesora.**



# 7. Wnioski z decyzji

---

Decyzja Prezesa UODO pokazuje, iż rzetelna analiza ryzyka oraz właściwy wybór i kontrola podmiotów przetwarzających stanowią kluczowe obowiązki każdego administratora danych osobowych.

Samo zawarcie umowy powierzenia, o ile nie jest ona w praktyce wykonywana i nałożone na nią obowiązki egzekwowane, nie ustrzeże przed naruszeniami RODO. Brak nadzoru i zabezpieczeń może skutkować poważnymi konsekwencjami finansowymi, tym większymi im większa skala naruszeń i większy podmiot ich dokonujący.



## 8. Przestroga dla całego rynku

Wydana, choć nieprawomocna jeszcze, decyzja wobec McDonald's to ważny sygnał dla całego rynku – outsourcing usług i czynności przetwarzania danych osobowych nie zwalnia z odpowiedzialności.

Każda organizacja musi dbać o bezpieczeństwo danych na każdym etapie ich przetwarzania, niezależnie czy tego przetwarzania dokonuje samodzielnie, czy angażując do tego podmioty trzecie.



# Kontakt



**Mariusz Purgał**

Partner

[mariusz.purgal@kwkr.pl](mailto:mariusz.purgal@kwkr.pl)



**Anna Bartosiak**

Associate

[anna.bartosiak@kwkr.pl](mailto:anna.bartosiak@kwkr.pl)

## Zespół Compliance KWKR



**Paweł  
Zyskowski**



**Katarzyna  
Kanik**



**Justyna  
Staszkiwicz**



**Bartosz  
Bogusławski**



**Agata  
Baca**



**Alicja  
Łopacińska**