

Warszawa, 24 lipca 2025 r.

## **Rekordowa kara dla McDonald's Polska. Dlaczego audyt podmiotów przetwarzających dane to konieczność?**

Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył na McDonald's Polska karę rekordową – ponad 16,9 mln zł – oraz na firmę 24/7 Communication Sp. z o.o. 183 tys. zł za naruszenia przepisów RODO. To najwyższa w Polsce sankcja finansowa za kwestie związane z ochroną danych osobowych.

### **Przyczyna kary**

Sprawa dotyczyła systemu zarządzania grafikami pracowników, gdzie wskutek błędnej konfiguracji serwera dane takie jak PESEL, numery paszportów, godziny pracy i stanowiska zostały publicznie dostępne. UODO wykazał liczne poważne uchybienia, m.in.:

- brak analizy ryzyka,
- niewdrożenie odpowiednich zabezpieczeń technicznych i organizacyjnych,
- brak nadzoru nad podmiotem przetwarzającym (bez audytów i kontroli umowy),
- brak umowy dalszego powierzenia danych,
- nieuwzględnienie Inspektora Ochrony Danych w kluczowych działaniach,
- nieprawidłowe poinformowanie byłych pracowników o incydencie.

Co ważne (ale też potencjalnie kontrowersyjne), UODO uznał, że McDonald's odpowiada także za dane pracowników franczyzobiorców, co znacząco zwiększyło skalę naruszenia.

### **Dlaczego audyt i nadzór podmiotów przetwarzających dane są konieczne?**

Ta sytuacja pokazuje jasno, że sama umowa powierzenia przetwarzania danych osobowych nie wystarczy. Administrator danych ma prawny obowiązek aktywnie nadzorować działania swoich partnerów przetwarzających dane przez:

- przeprowadzanie regularnych audytów,
- kontrolę realizacji umów powierzenia,
- weryfikację stosowanych środków technicznych i organizacyjnych,
- współpracę z Inspektorem Ochrony Danych.

Brak takich działań może skutkować poważnymi konsekwencjami finansowymi, prawnymi i wizerunkowymi.

### **Co daje audyt podmiotów przetwarzających?**

- pozwala ocenić zgodność z RODO i wdrożone zabezpieczenia,
- minimalizuje ryzyko wycieków i incydentów,
- umożliwia wykazanie organowi nadzorcemu, że administrator wywiązuje się ze swoich obowiązków (zasada rozliczalności),
- umożliwia bieżące dostosowywanie polityk ochrony danych do zmieniających się wymagań prawnych.

**Rekomendacje dla firm**

Warto regularnie przeprowadzać audyty i kontrole podmiotów przetwarzających, z którymi współpracują, a także współpracować z ekspertami w zakresie ochrony danych. Zapobiega to sytuacjom takim jak u McDonald's, gdzie zaniedbania prowadziły do rekordowej kary. Lepiej działać prewencyjnie niż ponosić wielomilionowe kary i stratę reputacji.

**Rekordowa kara dla McDonald's Polska jest efektem poważnych zaniedbań w nadzorze nad podmiotem przetwarzającym dane oraz braku odpowiednich zabezpieczeń. Audyt i kontrola partnerów przetwarzających dane to dziś niezbędny element zgodności z RODO i ochrona przed takim ryzykiem.**

**Maria Lothamer** – ekspert ds. ochrony danych osobowych, Wiceprezes Zarządu w iSecure Sp. z o.o.