UODO ukarał McDonald’s najwyższą karą w historii branży gastronomicznej w Polsce

Kategoria: Aktualności
Opublikowano: wtorek, 22, lipiec 2025 14:43
Katarzyna Sekuła
Odsłony: 1597

Prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski, nałożył na McDonald’s Polska Sp. z o.o. kary o łącznej wysokości 16 932 657 zł za liczne naruszenia przepisów o ochronie danych osobowych. Sankcje obejmują trzy kary: 1 632 063 zł, 13 600 528 zł oraz 1 700 066 zł, a dodatkowo spółka otrzymała upomnienie za brak bezpośredniego powiadomienia byłych pracowników o incydencie bezpieczeństwa. W tej samej sprawie karę w wysokości 183 858 zł nałożono również na 24/7 Communication Sp. z o.o., czyli podmiot przetwarzający dane w imieniu McDonald’s (94 286 zł, 42 429 zł i 47 143 zł).

Sprawa dotyczyła ujawnienia danych osobowych pracowników McDonald’s i jego franczyzobiorców, które znalazły się w publicznie dostępnym katalogu. Plik zawierał wrażliwe informacje, takie jak imiona i nazwiska, numery PESEL, numery paszportów, miejsca i godziny rozpoczęcia i zakończenia pracy, liczby przepracowanych godzin, stanowiska oraz informacje o dniach wolnych.

Brak analizy ryzyka i niewystarczające zabezpieczenia

McDonald’s Polska powierzył zarządzanie grafikami pracy firmie 24/7 Communication, jednak zarówno administrator, jak i podmiot przetwarzający, nie przeprowadzili właściwej analizy ryzyka, nie wdrożyli odpowiednich środków bezpieczeństwa ani nie prowadzili regularnych testów zabezpieczeń. Naruszenie wynikało z błędnej konfiguracji serwera, która umożliwiła nieautoryzowany podgląd bazy danych z modułu grafików.

UODO wskazał, że McDonald’s jako administrator nie miał dostępu do panelu administracyjnego modułu, a jednocześnie nie sprawował należytego nadzoru nad 24/7 Communication, co stanowi naruszenie art. 28 RODO. Co więcej, 24/7 Communication korzystała z usług kolejnego podwykonawcy, nie mając podpisanej umowy podpowierzenia, co jest sprzeczne z przepisami art. 28 ust. 4 i 9 RODO.

Niewłaściwy zakres danych i brak minimalizacji

Kontrola UODO wykazała również, że system grafików gromadził nadmiarowe dane, takie jak PESEL czy numery paszportów, które nie były niezbędne do ewidencjonowania czasu pracy. Dopiero po incydencie zostały one zastąpione mniej wrażliwymi numerami identyfikacyjnymi, co – zdaniem UODO – jest zgodne z zasadą minimalizacji danych wynikającą z art. 5 ust. 1 lit. c RODO.

Brak bezpośredniego zawiadomienia pracowników

Chociaż McDonald’s powiadomił osoby dotknięte naruszeniem, były to głównie komunikaty prasowe, które – w ocenie UODO – nie stanowią bezpośredniego zawiadomienia, do czego administrator był zobowiązany w przypadku wysokiego ryzyka naruszenia praw i wolności osób fizycznych.

Odpowiedzialność wobec pracowników franczyzobiorców

Prezes UODO uznał, że McDonald’s pełnił rolę administratora danych nie tylko wobec własnych pracowników, ale także wobec pracowników franczyzobiorców, ponieważ to spółka decydowała o funkcjonalności modułu grafików, zakresie gromadzonych danych oraz wyborze podmiotów przetwarzających.

Ostateczne rozstrzygnięcie UODO w tej sprawie stanowi wyraźny sygnał dla innych firm działających w

Polsce – zarówno dużych międzynarodowych marek, jak i mniejszych przedsiębiorstw. Organ nadzorczy przypomina, że obowiązek ochrony danych osobowych nie kończy się na podpisaniu umowy z podmiotem przetwarzającym. Kluczowe jest stałe monitorowanie procesów, weryfikowanie dostawców usług IT oraz wdrażanie realnych mechanizmów bezpieczeństwa. W przeciwnym razie, konsekwencje finansowe i wizerunkowe mogą być równie dotkliwe jak te, z którymi musi zmierzyć się teraz McDonald’s Polska.

Źródło: UODO