Warszawa, dn. 29.01.2026 r.

Ile kosztuje błędne wysłanie maila? O karach UODO za błędne wysłanie wiadomości.

Jedno kliknięcie za dużo, literówka w adresie e-mail czy pośpiech przy wysyłaniu dokumentów i gotowe. Umowa, faktura czy formularz z danymi osobowymi trafia do niewłaściwego odbiorcy. To jeden z najczęstszych scenariuszy naruszeń ochrony danych osobowych, z jakimi spotykamy się w naszej pracy.
Choć takie błędy zazwyczaj mają charakter nieumyślny, ich skutki mogą być bardzo poważne. Wysłanie wiadomości e-mail na niewłaściwy adres oznacza ujawnienie danych osobowych osobie nieuprawnionej. A to już wystarczy, by mówić o naruszeniu RODO niezależnie od tego, czy doszło do realnego nadużycia danych, czy „tylko" do zapoznania się z nimi przez niepowołanego odbiorcę.
Praktyka Urzędu Ochrony Danych Osobowych pokazuje, że tego rodzaju incydenty nie są bagatelizowane. Nawet pojedyncza, przypadkowa wysyłka maila może rodzić po stronie administratora konkretne obowiązki, a ich zaniechanie realne konsekwencje finansowe.
Urząd Ochrony Danych Osobowych (UODO) wydaje decyzje nakładające kary finansowe za naruszenia RODO, w tym za przypadki, gdy dane osoby fizycznej zostały ujawnione przez przesłanie e-maila na nieprawidłowy adres lub do nieuprawnionej osoby. Poniżej przedstawiam przykłady kar nałożonych przez Prezesa Urzędu Ochrony Danych i ich konkretne wartości:

1. **282.960 zł** (słownie: dwieście osiemdziesiąt dwa tysiące dziewięćset sześćdziesiąt złotych) za niezgłoszenie Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia oraz niezawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą. W sprawie ENEA S.A. doszło do nieuprawnionego ujawnienia danych osobowych Klientki, obejmujących m.in. numer PESEL, dane identyfikacyjne i kontaktowe oraz informacje o zawartej umowie. Zakres ujawnionych danych pozwalał na jednoznaczną identyfikację osoby, której dane dotyczą. Administrator uznał naruszenie za obarczone niskim ryzykiem i odstąpił od zgłoszenia go Prezesowi UODO oraz od poinformowania Klientki, opierając się na założeniu, że odbiorca dokumentu był „uczciwym znalazcą". Ocena ta nie została jednak wykazana zgodnie z zasadą rozliczalności. (DKN.5131.6.2023).

2. **29 684,04 zł** (słownie: dwadzieścia dziewięć tysięcy sześćset osiemdziesiąt cztery złote cztery grosze) za niezgłoszenie Prezesowi Urzędu Ochrony Danych Osobowych naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osoby, której dane dotyczą oraz nieprzekazaniu tej osobie, w ramach skierowanego do niej zawiadomienia, adekwatnego opisu środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu

ochrony danych osobowych, w tym środków w celu zminimalizowania jego ewentualnych negatywnych skutków. W Szpitalu doszło do omyłkowego wydania osobie nieuprawnionej dokumentu zawierającego dane osobowe pacjenta w postaci Przedoperacyjnej Ankiety Anestezjologicznej. Informacja o możliwym naruszeniu trafiła do Prezesa UODO, który zwrócił się do Administratora o wyjaśnienia dotyczące przeprowadzenia analizy ryzyka oraz ewentualnego zgłoszenia naruszenia i poinformowania osoby, której dane dotyczą. Administrator wskazał, że incydent nie został zgłoszony w momencie jego wystąpienia, co uniemożliwiło jednoznaczną identyfikację zdarzenia. Jednocześnie Szpital poinformował, że zawiadomił pacjenta o naruszeniu oraz podjął działania organizacyjne wobec personelu. Naruszenie ochrony danych osobowych zostało zgłoszone Prezesowi UODO dopiero po wszczęciu postępowania administracyjnego, z przekroczeniem ustawowego terminu 72 godzin. Przekazane zawiadomienie dla osoby, której dane dotyczą, nie zawierało wszystkich informacji wymaganych przepisami RODO. (DKN.5131.6.2024).

3. **250.000** PLN (słownie: dwieście pięćdziesiąt tysięcy złotych) za niezawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych w terminie 24 godzin od wykrycia naruszenia danych osobowych oraz braku niezwłocznego powiadomienia o naruszeniu danych osobowych abonenta, którego dotyczyło naruszenie. W lutym 2022 r. do Prezesa UODO wpłynęła informacja od osoby trzeciej, która otrzymała pocztą elektroniczną umowę telekomunikacyjną Play dotyczącą innej osoby o tym samym nazwisku. Przesłana umowa zawierała pełen zakres danych osobowych, w tym numer PESEL oraz numer i serię dowodu osobistego. Prezes UODO zwrócił się do P4 Sp. z o.o. o wyjaśnienia dotyczące możliwego naruszenia ochrony danych osobowych oraz o ocenę obowiązku zgłoszenia naruszenia i zawiadomienia osoby, której dane dotyczą. Spółka wyjaśniła, że umowa została zawarta w Punkcie Obsługi Sprzedaży, a kopia dokumentów została automatycznie wysłana na adres e-mail wskazany przez klienta w umowie. Adres ten okazał się błędny, co klient zgłosił po zawarciu umowy, prosząc o jego usunięcie. Spółka wskazała, że wysyłka dokumentów nastąpiła zgodnie z danymi podanymi i podpisanymi przez klienta, a pracownik POS nie wyłączył opcji automatycznej wysyłki. Administrator uznał, że nie doszło do naruszenia danych osobowych, ponieważ korespondencja została wysłana na adres wskazany przez klienta, a do marca 2022 r. nie odnotowano zgłoszeń ani od klienta, ani od osoby trzeciej dotyczących nieuprawnionego dostępu do danych. W związku z brakiem zgłoszenia naruszenia Prezesowi UODO oraz niepowiadomieniem abonenta, w kwietniu 2022 r. Prezes UODO wszczął wobec Spółki postępowanie administracyjne. (DKN.5131.18.2022).

4. **4 053 173 zł** (słownie: cztery miliony pięćdziesiąt trzy tysiące sto siedemdziesiąt trzy złote) za niezawiadomienie o naruszeniu ochrony danych osobowych bez zbędnej zwłoki osób, których dane dotyczą. X. S.A. zgłosił Prezesowi UODO naruszenie ochrony danych osobowych, do którego doszło 30 czerwca 2022 r., polegające na błędnym przesłaniu dokumentów bankowych klientów do innego banku przez pracownika podmiotu

przetwarzającego dane na zlecenie Banku. Dokumenty zostały następnie zwrócone, jednak istniało prawdopodobieństwo, że zapoznali się z nimi pracownicy innego banku. Bank wskazał, że doszło do naruszenia poufności danych osobowych wielu klientów, obejmujących szeroki zakres informacji, w tym dane identyfikacyjne, adresowe, finansowe oraz dane dotyczące kredytów i nieruchomości. Administrator uznał, że ryzyko naruszenia praw i wolności klientów jest ograniczone z uwagi na obowiązek zachowania tajemnicy bankowej przez pracowników banku, wobec czego nie poinformował osób, których dane dotyczą. Po przeprowadzeniu postępowania wyjaśniającego Prezes UODO wszczął z urzędu postępowanie administracyjne w celu oceny czy Bank naruszył obowiązki wynikające z art. 34 ust. 1 i 2 RODO, dotyczące zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. (DKN.5131.1.2024).

Jak się zabezpieczyć przed karami za błędną wysyłkę?

1. **Sprawdź adresata** - zanim wyślesz e-mail z danymi osobowymi, zawsze upewnij się, że adres jest poprawny. Warto wprowadzić systemowe blokady wysyłki na nieznane lub niepotwierdzone adresy oraz podwójną weryfikację. Taka prosta procedura znacznie zmniejsza ryzyko przypadkowego ujawnienia danych osobom nieuprawnionym.

2. **Szkol pracowników** - regularne szkolenia z zakresu ochrony danych osobowych i procedur bezpieczeństwa uświadamiają pracowników, jakie konsekwencje mogą wyniknąć z błędnej wysyłki. Dzięki temu są oni bardziej świadomi i ostrożni w codziennej pracy, co minimalizuje ryzyko pomyłek.

3. **Miej procedury reagowania** - każda firma powinna mieć gotowy plan postępowania na wypadek błędnej wysyłki. Ważne jest szybkie ograniczenie skutków incydentu, np. cofnięcie e-maila, kontakt z odbiorcą i powiadomienie osób, których dane dotyczą. Jeśli ryzyko jest wysokie, należy też niezwłocznie zgłosić naruszenie do UODO.

4. **Wykorzystaj zabezpieczenia techniczne** - systemy pocztowe i CRM oferują funkcje kontrolujące wysyłkę danych, np. blokadę korespondencji zawierającej dane osobowe na zewnętrzne adresy, szyfrowanie wiadomości czy opcję cofnięcia wysyłki w krótkim czasie. Takie narzędzia stanowią dodatkową warstwę ochrony obok procedur wewnętrznych.

5. **Minimalizuj ilość przesyłanych danych** - zasada „minimalizacji danych" oznacza, że w wiadomości wysyłamy tylko niezbędne informacje. Dzięki temu w razie pomyłki zakres ujawnionych danych jest ograniczony, co zmniejsza ryzyko naruszenia RODO i ewentualnej kary.

Gabriela Tokarska - młodsza specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.