Warszawa, 05.08.2025

5 najczęstszych błędów wykrywanych podczas audytów ochrony danych

WSTĘP

Audyt RODO w firmie? Tych 5 błędów unikaj jak ognia!

Audyt ochrony danych osobowych – już samo to sformułowanie u wielu przedsiębiorców wywołuje szybsze bicie serca. Kojarzy się z kontrolą, stresem i szukaniem dziury w całym. A co, jeśli powiemy Ci, że audyt to tak naprawdę Twój najlepszy przyjaciel w dbaniu o bezpieczeństwo firmy? To szansa, żeby spojrzeć na swoje procesy z boku i wyłapać błędy, zanim znajdzie je Prezes Urzędu Ochrony Danych Osobowych (UODO).

Przez lata pomagaliśmy firmom przechodzić przez audyty RODO. Zauważyliśmy, że pewne błędy powtarzają się z zadziwiającą regularnością, niezależnie od branży czy wielkości organizacji. Dziś dzielimy się listą 5 najczęstszych potknięć. Sprawdź, czy nie dotyczą one także Twojej organizacji!

1. Dokumentacja? Jaka dokumentacja?

To absolutny klasyk. Pytamy w firmie o dokumentację ochrony danych, a w odpowiedzi zapada niezręczna cisza. Brak Polityki Bezpieczeństwa, brak Rejestru Czynności Przetwarzania, brak procedur… Krótko mówiąc: dokumentacyjny Dziki Zachód.

- **Dlaczego to błąd?** RODO wprost wymaga posiadania i prowadzenia określonej dokumentacji. To nie jest „papierek dla papierka", ale mapa Twoich danych. Pokazuje, jakie dane zbierasz, po co to robisz, gdzie je trzymasz i jak je chronisz. Bez niej działasz po omacku i nie jesteś w stanie udowodnić, że spełniasz obowiązki. To też jedno z pierwszych pytań, które Prezes Urzędu Ochrony Danych Osobowych zada podczas ewentualnej kontroli.
- **Jak to naprawić?** Zacznij od podstaw: stwórz Rejestr Czynności Przetwarzania. To fundament. Opisz w nim kluczowe procesy w firmie, np. rekrutację, obsługę klientów czy wysyłkę newslettera. Potem stopniowo buduj resztę dokumentacji. W pierwszej kolejności to Polityka Ochrony Danych Osobowych. firmowa "konstytucja" określająca, kto jest odpowiedzialny za dane i jakie są ogólne zasady ich ochrony. Równie ważne są szczegółowe instrukcje, czyli procedury, które krok po kroku wyjaśniają, jak postępować w konkretnych sytuacjach – na przykład, co robić, gdy klient zażąda usunięcia swoich danych lub gdy pracownik zgubi służbowy laptop. Niezbędne jest również prowadzenie dodatkowych ewidencji, takich jak rejestr osób upoważnionych do przetwarzania danych, rejestr naruszeń. Nie można zapomnieć o proaktywnym podejściu, czyli przeprowadzeniu analizy ryzyka, aby

zidentyfikować potencjalne zagrożenia dla danych i zaplanować, jak im przeciwdziałać. W tej kategorii mieszczą się również absolutnie kluczowe procedury IT, które stanowią techniczny kręgosłup bezpieczeństwa: od zarządzania dostępami (czyli jak sprawnie nadawać i odbierać uprawnienia pracownikom), przez tworzenie i odtwarzanie kopii zapasowych (backupów), politykę silnych haseł, aż po procedury aktualizacji oprogramowania i bezpiecznego usuwania danych z wycofywanych komputerów. Bez tych technicznych wytycznych nawet najlepsze zapisy ogólne pozostaną tylko na papierze. Całość uzupełniają klauzule informacyjne – przejrzyste komunikaty umieszczane wszędzie tam, gdzie zbierasz dane, np. na stronie internetowej czy w formularzach rekrutacyjnych, które informują ludzi o ich prawach i celach przetwarzania.

2. Pracownik (nie)przeszkolony, czyli najsłabsze ogniwo

Możesz mieć najlepsze systemy, najdroższe oprogramowanie antywirusowe i szafy pancerne na dokumenty. Wystarczy jednak jeden nieświadomy pracownik, który kliknie w podejrzany link, wyniesie z firmy pendrive z danymi klientów albo zostawi na biurku niezablokowany komputer lub wyśle zbiorczego maila do wielu odbiorców bez funkcji UDW.

- **Dlaczego to błąd?** Człowiek jest i zawsze będzie kluczowym elementem systemu bezpieczeństwa. Brak regularnych, praktycznych szkoleń z ochrony danych to proszenie się o kłopoty. Audytorzy od razu to wyłapią, pytając pracowników o podstawowe zasady, np. politykę czystego biurka.
- **Jak to naprawić?** Organizuj szkolenia! Nie raz na trzy lata, ale regularnie. Mów prostym językiem, używaj przykładów z życia i testuj wiedzę. Pokaż, że hasło „Firma123!" to zły pomysł, a na maile od „nieznanych nadawców lub z podejrzanymi linkami" się nie odpowiada.

3. „Zaprzyjaźniona" księgowość i inne demony, czyli brak umów powierzenia

„Księgowość prowadzi nam zaprzyjaźniona firma pani Kasi, znamy się od lat". To świetnie, ale czy pani Kasia ma z Tobą podpisaną umowę powierzenia przetwarzania danych? A co z firmą od hostingu, agencją marketingową czy dostawcą oprogramowania do faktur?

- **Dlaczego to błąd?** Jeśli jakikolwiek podmiot zewnętrzny ma dostęp do danych osobowych, za które odpowiadasz (np. dane pracowników, klientów), musisz mieć z nim podpisaną umowę powierzenia przetwarzania danych. To ona reguluje, co ten podmiot może robić z danymi i jak ma je chronić. Bez niej to Ty ponosisz pełną odpowiedzialność za jego ewentualne wpadki. Dodatkowo, musisz udokumentować weryfikację kontrahenta pod kątem jego zgodności z przepisami RODO. Powinieneś współpracować wyłącznie z podmiotami gwarantującymi przetwarzanie powierzonych danych osobowych zgodnie z obowiązkami wynikającymi z Rozporządzenia.

- **Jak to naprawić?** Zrób listę swoich dostawców i partnerów.
  Sprawdź, którzy z nich mają dostęp do danych. Upewnij się, że z każdym z nich masz podpisaną poprawną umowę powierzenia. Skonsultuj to z Działem Prawnym lub audytorem.

4. Komputer prezesa na hasło „admin1" i inne grzechy techniczne

Audyt to nie tylko dokumenty, ale też szybki rzut oka na codzienne praktyki. Co widzi audytor? Komputery bez haseł, karteczki z hasłami przyklejone do monitorów, dokumenty z danymi leżące na wierzchu w ogólnodostępnym miejscu, brak aktualnego oprogramowania antywirusowego.

- **Dlaczego to błąd?** RODO wymaga wdrożenia „odpowiednich środków technicznych i organizacyjnych", aby zapewnić bezpieczeństwo danych. Hasło „123456" takim środkiem na pewno nie jest. To podstawowa higiena cyfrowa, której brak jest sygnałem, że w firmie nikt nie traktuje bezpieczeństwa poważnie.
- **Jak to naprawić?** Wprowadź politykę silnych haseł. Wymuś automatyczne blokowanie ekranu po kilku minutach bezczynności. Szyfruj dyski w laptopach. Upewnij się, że antywirus jest aktualny, a systemy regularnie aktualizowane. To proste kroki, które ogromnie podnoszą poziom bezpieczeństwa.

5. „Chcę usunąć swoje dane!" – czyli panika w dziale obsługi klienta

Dzwoni klient i mówi, że na podstawie RODO żąda usunięcia wszystkich swoich danych. Co robi pracownik? Najczęściej wpada w panikę, bo nie wie, co ma zrobić, do kogo to przekazać i czy w ogóle może to zrobić.

- **Dlaczego to błąd?** Każda osoba, której dane przetwarzasz, ma określone prawa: prawo do dostępu do danych, ich sprostowania, usunięcia („prawo do bycia zapomnianym") itd. Twoja firma musi być gotowa, aby te prawa zrealizować w ustawowym terminie (zazwyczaj miesiąc). Ignorowanie takich żądań to prosta droga do skargi do UODO.
- **Jak to naprawić?** Stwórz prostą ścieżkę postępowania na wypadek otrzymania takiego żądania. Każdy pracownik mający kontakt z klientem musi wiedzieć, co robić i komu natychmiast przekazać sprawę. Dodaj do polityki ochrony danych osobowych procedurę obsługi wniosków podmiotów danych.

Audyt to nie koniec świata!

Jak widzisz, większość audytowych wpadek nie wynika ze złej woli, ale z przeoczenia i braku świadomości. Dobra wiadomość jest taka, że wszystkie te błędy da się stosunkowo prosto naprawić.

Zastanów się też, czy w Twojej organizacji nie jest wymagane lub po prostu przydatne powołanie Inspektora Ochrony Danych, który będzie stał na straży całego systemu.

Pamiętaj, że to nie jest tworzenie dokumentów dla samych dokumentów. To budowanie realnego systemu bezpieczeństwa. Traktuj ochronę danych nie jak przykry obowiązek, ale jak inwestycję w zaufanie klientów i stabilność Twojego biznesu. Zaufanie to dziś jedna z najcenniejszych walut.

Maciej Łukaszewicz, Radca prawny, Specjalista ds. ochrony danych osobowych