Warszawa, dn. 3.02.2026 r.

5 najczęstszych błędów w ochronie danych osobowych i jak ich unikać (praktyczne przykłady z audytów)

Ochrona danych osobowych to temat, który wraca regularnie – ale dziś wraca ze zdwojoną siłą. W ostatnich miesiącach kolejne firmy otrzymują wysokie kary za niedopilnowanie podstawowych obowiązków wynikających z RODO. Co ważne – w większości przypadków nie chodzi o spektakularne cyberataki, ale o codzienne zaniedbania.

Podczas audytów widzę powtarzające się błędy, które można szybko naprawić – zanim zrobi to organ nadzorczy. Poniżej przedstawiam 5 najczęstszych problemów oraz konkretne przykłady z firm, które audytowałam.

Brak kontroli nad dostępami do danych

Błąd: dostęp do danych osobowych ma zbyt wiele osób – bez uzasadnienia i bez regularnego przeglądu uprawnień.

Case z audytu

W jednej z firm usługowych (ok. 150 pracowników) okazało się, że dostęp do systemu kadrowego ma nie tylko dział HR, ale też kierownicy magazynu i kilka osób z działu sprzedaży. Powód? „Tak zostało po wdrożeniu systemu". Nikt nigdy nie przeprowadził przeglądu dostępów, mimo że w systemie znajdowały się dane wrażliwe.

Jak uniknąć?

- wdrożenie zasady minimalnych uprawnień,
- przegląd dostępów co najmniej raz na pół roku,
- szybkie odbieranie dostępów po zmianie stanowiska lub odejściu pracownika.

Dokumentacja „dla papieru", która nie odzwierciedla rzeczywistości

Błąd: firma posiada politykę ochrony danych osobowych, ale jest ona nieaktualna lub nie jest stosowana w praktyce.

Case z audytu

Podczas audytu w firmie handlowej znalazłam procedurę zgłaszania naruszeń, która zakładała centralną rolę dla inspektora ochrony danych przy obsłudze naruszeń (co w obecnym stanie faktycznym jest problematyczne i może wiązać się z interwencją ze strony UODO). Co więcej, nikt z pracowników nie wiedział, że taka procedura istnieje. W razie incydentu firma nie byłaby w stanie zareagować w wymaganym terminie 72 godzin.

Jak uniknąć?

- aktualizacja dokumentacji dotyczącej ochrony danych osobowych minimum raz w roku,
- krótkie szkolenia wdrożeniowe zamiast „regulaminów do podpisu",
- testowanie procedur w praktyce (np. symulacje incydentu).

Brak umów powierzenia z podwykonawcami

Błąd: dane są przekazywane firmom zewnętrznym (np. IT, kadry, marketing), ale brak zawartych formalnych umów powierzenia przetwarzania danych osobowych.

Case z audytu

W jednej z audytowanych organizacji outsourcing IT miał pełny dostęp do serwerów z danymi klientów. Firma nie miała podpisanej umowy powierzenia, bo „przecież współpracujemy od lat". To jeden z najczęstszych powodów kar – organy nadzorcze szczególnie mocno kontrolują relacje z procesorami.

Jak uniknąć?

- lista wszystkich podmiotów przetwarzających dane,
- podpisanie umów powierzenia zgodnych z art. 28 RODO,
- okresowa weryfikacja dostawców (czy spełniają wymagania bezpieczeństwa).

Przetwarzanie danych „na zapas" – zbyt dużo i zbyt długo

Błąd: firmy zbierają więcej danych niż potrzebują i przechowują je latami bez podstawy prawnej.

Case z audytu

W firmie rekrutacyjnej przechowywano CV kandydatów sprzed 8 lat, mimo że procesy były zamknięte. Dane leżały w folderach „na wszelki wypadek". To klasyczny przykład naruszenia zasady minimalizacji i ograniczenia przechowywania.

Jak uniknąć?

- ustalenie okresów retencji danych,
- automatyczne usuwanie lub anonimizacja danych po zakończeniu celu związanego z ich wykorzystywaniem (cel został zrealizowany),
- pytanie „czy naprawdę potrzebujemy tej informacji?".

Niedostateczne zabezpieczenia techniczne – szczególnie w małych firmach

Błąd: brak podstawowych zabezpieczeń (np. szyfrowania, wykonywania kopii zapasowych).

Case z audytu

W jednej z firm transportowych dostęp do poczty służbowej był zabezpieczony wyłącznie hasłem typu „Firma2023". Nie było uwierzytelniania dwuskładnikowego. Po wejściu do skrzynki można było znaleźć skany dowodów osobistych klientów przesyłane mailem. To najprostsza droga do tego, by UODO nałożyło karę finansową...

Jak uniknąć?

- Dwuetapowe uwierzytelnianie wszędzie, gdzie jest to możliwe,
- szyfrowanie laptopów i nośników danych,
- wykonywanie kopii zapasowych i regularne testy odtwarzania,
- zakaz przesyłania wrażliwych danych mailem bez zabezpieczeń.

Większość błędów to codzienne zaniedbania

Najczęstsze problemy w ochronie danych osobowych nie wynikają ze złej woli – tylko z braku praktycznych procesów, kontroli i aktualizacji. A kary? Są coraz bardziej realne – szczególnie za podstawowe braki: dokumentację, umowy powierzenia, dostęp do danych czy zabezpieczenia IT.
Jeśli chcesz mieć pewność, że Twoja firma nie popełnia tych błędów – warto zrobić audyt zanim zrobi go Urząd Ochrony Danych Osobowych.

Olga Skotnicka – ekspertka ds. ochrony danych osobowych w iSecure Sp. z o.o.