Warszawa, 12.08.2025 r.

Trendy w ochronie danych osobowych – na co dziś zwracają uwagę firmy i regulatorzy?

Ochrona danych osobowych to już nie tylko compliance, ale również element budowania zaufania, przewagi konkurencyjnej i odpowiedzialnego zarządzania ryzykiem.

W ostatnich latach, a szczególnie miesiącach, ochrona danych osobowych przeszła istotną transformację. Przestała być traktowana wyłącznie jako wymóg regulacyjny, który trzeba „odhaczyć" w ramach działań compliance. Dziś dane osobowe – zwłaszcza w środowisku cyfrowym – są jednym z najcenniejszych zasobów organizacji, a sposób, w jaki są zbierane, przetwarzane i chronione, staje się bezpośrednim wyznacznikiem dojrzałości operacyjnej i etycznej firmy.

Zaufanie klientów buduje się dziś nie tylko na podstawie jakości usług, ale również na transparentności i odpowiedzialności w obchodzeniu się z danymi. Coraz więcej osób fizycznych jest świadomych swoich praw, a każda wpadka w obszarze danych osobowych (np. wyciek, nieuprawniony kontakt, błędna decyzja algorytmu) może bezpośrednio przełożyć się na utratę reputacji, klientów i przewagi konkurencyjnej.

Zarządzanie ryzykiem związanym z danymi zaczęło obejmować nie tylko działania techniczne, ale również strategiczne podejście do:

- planowania kampanii marketingowych,
- rozwoju aplikacji i platform cyfrowych,
- kształtowania relacji z partnerami (np. transfery danych),
- rekrutacji, onboardingu i monitorowania pracowników,
- wdrażania systemów AI i automatyzacji procesów.

Dobrze zaprojektowane podejście do ochrony danych to dziś również **przewaga w relacjach B2B** – wiele podmiotów już na etapie wyboru dostawcy usług weryfikuje jego podejście do RODO, poziom zabezpieczeń oraz procesy zarządzania incydentami. Coraz częściej spotykamy się z sytuacją, w której brak transparentnych procedur lub przestarzałe dokumenty RODO mogą przesądzić o wykluczeniu z przetargu lub współpracy.

W ostatnim czasie obserwujemy kilka wyraźnych trendów, które pokazują, w którym kierunku zmierza rynek – zarówno od strony praktyki biznesowej, jak i podejścia organów nadzorczych.

Regulatorzy w Polsce i Europie zaczynają coraz bardziej stanowczo egzekwować rzeczywistą zgodność z przepisami, a nie tylko deklaratywne „wdrożenie RODO". Jednocześnie firmy, które wcześniej traktowały ochronę danych jako element drugorzędny, dziś coraz częściej włączają kwestie prywatności do procesów zarządzania produktem, marketingiem i strategią rozwoju.

Z jednej strony widzimy intensyfikację kontroli, sankcji oraz wyraźne stanowiska organów (m.in. w zakresie zgód marketingowych, danych biometrycznych, czy transferów do państw trzecich). Z drugiej – rośnie presja rynkowa, wynikająca z oczekiwań klientów, partnerów i inwestorów, by organizacje działały etycznie, odpowiedzialnie i zgodnie z zasadą privacy by design.

W tym kontekście wyraźnie wyodrębniają się nowe **trendy**, które warto znać – nie tylko po to, by uniknąć ryzyk prawnych, ale przede wszystkim by lepiej dopasować się do oczekiwań rynku i wzmacniać swoją pozycję biznesową.

1. Koniec „papierowego RODO" – rośnie nacisk na realne działania

Jeszcze kilka lat temu wiele organizacji traktowało RODO głównie jako wymóg formalny – sporządzano pakiet dokumentacji (polityki, procedury, rejestry, klauzule), który trafiał do segregatora i... na tym często kończyło się wdrożenie. Dziś to podejście przestaje być akceptowalne – ani przez klientów, ani przez regulatorów.

Co się zmienia?

Zarówno UODO, jak i europejskie organy nadzorcze coraz częściej w swoich działaniach kontrolnych i decyzjach nakładających kary wskazują wprost, że sama dokumentacja – nawet kompletna i aktualna – nie wystarcza. Liczy się to, **czy przepisy i procedury faktycznie działają w praktyce**, są znane pracownikom i stosowane na co dzień.

Przykłady działań, których dziś oczekują regulatorzy:

- **Realna egzekucja praw osób fizycznych:** Czy zgłoszenia są obsługiwane w terminach? Czy organizacja potrafi sprawnie zidentyfikować, gdzie znajdują się dane osoby, która np. żąda ich usunięcia? Czy odpowiedzi na wnioski są merytoryczne i konkretne, czy tylko ogólnikowe?
- **Funkcjonujący system zarządzania incydentami:** Czy zgłoszenia naruszeń są rejestrowane? Czy wiadomo, kto je analizuje i jak zapada decyzja o ewentualnym zgłoszeniu do UODO? Czy przeprowadzana jest analiza przyczyn i wdrażane są środki naprawcze?
- **Szkolenia i podnoszenie świadomości:** Czy pracownicy faktycznie wiedzą, jak chronić dane osobowe w swojej codziennej pracy? Czy wiedzą, jak reagować na podejrzenie incydentu? Czy szkolenia są dopasowane do roli (np. inne dla działu sprzedaży, inne dla HR), czy też są tylko ogólnym webinarem raz na trzy lata?
- **Bieżąca aktualizacja rejestrów i dokumentacji:** Czy rejestr czynności przetwarzania faktycznie odzwierciedla działalność organizacji, czy też opisuje „stan z 2019 roku"? Czy ktoś go weryfikuje przy wdrażaniu nowych projektów, systemów IT, procesów marketingowych?

Co to oznacza dla organizacji?

Warto zweryfikować, które procedury istnieją tylko „na papierze", a które są rzeczywiście wdrożone i zrozumiane w organizacji. Firmy zaczynają wdrażać audyty wewnętrzne, testy socjotechniczne i praktyczne szkolenia, a nie tylko „odhaczać" obowiązki. W praktyce oznacza to potrzebę przejścia od „compliance teoretycznego" do **compliance operacyjnego** – czyli takiego, który funkcjonuje i reaguje w czasie rzeczywistym.

Firmy, które chcą uniknąć ryzyk prawnych, reputacyjnych i finansowych, nie mogą już traktować ochrony danych jako zadania do wykonania raz na kilka lat. Należy ją zintegrować z codziennym zarządzaniem, kulturą organizacyjną i strategią IT. Inaczej mówiąc: RODO musi „żyć" w organizacji

2. Wzrost znaczenia zarządzania zgodami i preferencjami użytkowników

Zmieniające się otoczenie regulacyjne, w tym wejście w życie nowego **Prawa komunikacji elektronicznej (PKE)**, jeszcze bardziej zaostrzyło wymagania w zakresie uzyskiwania zgód marketingowych i informowania użytkowników o przetwarzaniu ich danych w kanałach cyfrowych.

Co się zmienia w praktyce?

O ile wcześniej wiele firm opierało komunikację marketingową na tzw. zgodach zbiorczych (np. „zgadzam się na kontakt drogą elektroniczną i telefoniczną"), dziś to podejście nie tylko bywa kwestionowane przez organy nadzorcze, ale coraz częściej spotyka się też z oporem odbiorców. Użytkownicy oczekują jasnego rozróżnienia celów przetwarzania (np. newsletter, kontakt telefoniczny, personalizacja treści) oraz kanałów komunikacji (e-mail, SMS, telefon, push), i chcą nimi indywidualnie zarządzać.

W odpowiedzi na te oczekiwania i nowe przepisy, firmy wdrażają tzw. **preference centers** – dedykowane panele lub formularze, które umożliwiają użytkownikom pełne zarządzanie zgodami i preferencjami marketingowymi. Dobrym standardem staje się:

- możliwość wyboru **konkretnych typów komunikatów** (np. nowości, promocje, zaproszenia na wydarzenia),
- rozdzielenie zgód na różne kanały (np. osobne zgody na e-mail, SMS, telefon),
- przypomnienie użytkownikowi o jego aktualnych ustawieniach i łatwe ich zmienianie,
- rejestrowanie wszystkich działań użytkownika w systemie CRM (jako dowód zgodności z RODO i PKE).

3. Uwaga na transfery danych – zacieśnienie kontroli po Schrems II

Wyrok Trybunału Sprawiedliwości UE w sprawie **Schrems II** z 2020 roku unieważnił mechanizm **Privacy Shield** jako podstawę transferu danych do USA, wyraźnie podkreślając, że sam fakt zawarcia umowy lub umieszczenia danych w chmurze nie wystarcza, by uznać transfer za zgodny z RODO.

Choć od wyroku minęło już kilka lat, to jego **praktyczne skutki są coraz silniej odczuwalne** – zarówno w postępowaniach nadzorczych, jak i w oczekiwaniach kontrahentów oraz praktykach dużych klientów korporacyjnych.

Co to oznacza w praktyce?

Dziś, jeśli organizacja przekazuje dane osobowe do państwa spoza EOG (np. USA, Indie, Izrael), musi spełnić dwa warunki:

1. Mieć odpowiednią podstawę prawną transferu, np. standardowe klauzule umowne (SCC),
2. Dokonać tzw. Transfer Impact Assessment (TIA) – czyli ocenić, czy w kraju odbiorcy dane będą realnie chronione w stopniu zbliżonym do UE.

Czego wymagają regulatorzy i partnerzy B2B?

- **Dokumentacja TIA** powinna być przejrzysta, zawierać ocenę zagrożeń (np. ryzyko dostępu służb publicznych), analizę systemu prawnego kraju odbiorcy oraz środki techniczne i organizacyjne zastosowane po stronie odbiorcy.
- **Dodatkowe zabezpieczenia**, takie jak szyfrowanie end-to-end, pseudonimizacja, ograniczenia dostępowe (np. dostęp tylko z UE) – coraz częściej są traktowane jako warunek konieczny.
- **Transparentność wobec osób, których dane dotyczą** – konieczność wskazania w polityce prywatności do jakich państw dane są przekazywane i dlaczego

Co robią firmy?

- Weryfikują dostawców chmurowych i IT pod kątem lokalizacji danych i mechanizmów zabezpieczających transfery.
- Wdrażają procedury TIA oraz angażują zespoły prawne i bezpieczeństwa IT do ich cyklicznej aktualizacji.
- W przypadku wątpliwości – **rezygnują z transferu danych poza EOG**, szukając europejskich alternatyw lub decydując się na przechowywanie danych lokalnie.

Wniosek: kontrola nad przepływem danych to nie tylko kwestia prawa – to obowiązek biznesow

Brak dokumentacji TIA lub nieprzejrzyste mechanizmy transferowe mogą być dziś powodem nie tylko interwencji regulatora, ale także utraty kontraktu z klientem korporacyjnym, który oczekuje pełnej zgodności z RODO

4. Dane biometryczne i monitoring – więcej ograniczeń niż się wydaje

Wraz z rozwojem technologii coraz więcej firm sięga po **narzędzia biometryczne** – takie jak logowanie odciskiem palca, systemy rozpoznawania twarzy, analiza wzorców głosu czy monitoring wizyjny z funkcją detekcji i rozpoznawania osób. Motywacją zwykle jest wygoda, automatyzacja procesów lub zwiększenie bezpieczeństwa.

Jednak dane biometryczne nie są „zwykłymi danymi osobowymi". Zgodnie z RODO (art. 9 ust. 1) są to **dane szczególnej kategorii**, co oznacza, że ich przetwarzanie jest co do zasady **zabronione**, chyba że zachodzi jedna z wyjątkowych podstaw legalności wymienionych w przepisach.

Dlaczego dane biometryczne są tak problematyczne?

- **Są trwałe i niezmienne.** W przeciwieństwie do hasła czy karty dostępu, odcisku palca czy twarzy nie da się zmienić po „wycieku".
- **Mogą mieć wysoką wartość identyfikacyjną i umożliwiać śledzenie danej osoby**, także w sposób zautomatyzowany i niejawny.
- **Mogą być pozyskiwane w sposób ukryty**, bez wiedzy i wyraźnej świadomości osoby (np. analiza obrazu CCTV z funkcją AI).

Monitoring wizyjny – zakres zastosowania też nie jest nieograniczony

Firmy coraz częściej wdrażają systemy CCTV nie tylko w przestrzeniach wspólnych (np. recepcjach, magazynach), ale również:

- w pokojach biurowych,
- w pomieszczeniach socjalnych,
- a nawet przy stanowiskach pracy.

Tymczasem monitoring może być stosowany wyłącznie, gdy jest **niezbędny do realizacji uzasadnionych celów administratora**, a cele te nie mogą być osiągnięte w inny, mniej inwazyjny sposób. RODO (art. 5 i 6) oraz przepisy krajowe (np. kodeks pracy) jasno ograniczają jego dopuszczalność

Ryzyka praktyczne:

- Naruszenie zasady minimalizacji i proporcjonalności – zbyt szeroki zakres monitoringu lub analiza biometrii „na zapas".
- Brak rzetelnego DPIA (oceny skutków dla ochrony danych) – co jest wymagane zawsze w przypadku biometrii lub zautomatyzowanej analizy obrazu.
- Błędne poleganie na zgodzie – wiele firm nie rozumie, że zgoda pracownika lub użytkownika, który nie ma wyboru, nie spełnia wymogów RODO.
- Brak transparentności – niedostateczne informowanie o celach, czasie przechowywania, odbiorcach nagrań lub o działaniu systemów biometrycznych.

Co powinny zrobić firmy?

1. Unikać danych biometrycznych, jeśli tylko jest to możliwe. W większości przypadków istnieją mniej inwazyjne alternatywy (np. karta dostępu, kod).
2. Przeprowadzać DPIA (ocenę skutków) przed wdrożeniem systemów biometrycznych i monitoringu.
3. Zapewniać przejrzystość i wybór. Użytkownicy muszą być poinformowani, a zgoda nie może być warunkiem korzystania z usługi.
4. Wyznaczyć jasny cel, zakres i czas przechowywania danych. Nie wolno „na wszelki wypadek" gromadzić danych biometrycznych.
5. Regularnie audytować systemy i dokumentację – i dostosowywać je do zmieniających się przepisów i stanowisk organów.

5. Ochrona danych w aplikacjach mobilnych i AI

Rozwój aplikacji mobilnych oraz coraz powszechniejsze wykorzystanie narzędzi opartych na sztucznej inteligencji zmienia sposób, w jaki dane osobowe są zbierane, analizowane i wykorzystywane. Zmieniają się też oczekiwania regulatorów i użytkowników – nacisk kładziony jest nie tylko na bezpieczeństwo danych, ale również na **transparentność, celowość oraz uczciwość przetwarzania**.

Aplikacja mobilna to dziś nie tylko „interfejs użytkownika" – to także zbieranie danych o lokalizacji, zachowaniach, interakcjach, preferencjach. W połączeniu z AI tworzy to potężne środowisko analityczne, które – jeśli nie zostanie odpowiednio uregulowane – stwarza realne ryzyko naruszenia prywatności.

Dla DPO i zespołów IT oznacza to konieczność:

a) przejrzystych polityk prywatności w aplikacjach tj. użytkownik musi otrzymać informacje **już przy pierwszym uruchomieniu aplikacji**, a nie tylko na stronie internetowej, w sposób zwięzły i zrozumiały (a nie 12-stronicowy PDF), w języku interfejsu aplikacji i oczywiście z możliwością łatwego cofnięcia zgody lub zmiany ustawień.
b) rozdzielenia niezbędnych funkcji od marketingowych, ponieważ w aplikacjach często dane są zbierane nie tylko po to, by świadczyć usługę, ale też m. in. do analizy zachowań użytkownika (np. przez SDK Google/Facebooka), do remarketingu czy do tworzenia profili (np. „użytkownicy zainteresowani zdrowiem psychicznym").

Co to oznacza?

- funkcje „konieczne” (np. logowanie, działanie koszyka) **nie mogą być uzależnione od zgody**, ale funkcje „dodatkowe” już tak – i muszą być domyślnie wyłączone (zgoda typu opt-in),
- zewnętrzne narzędzia analityczne i reklamowe muszą być odpowiednio skonfigurowane i uwzględnione w dokumentacji RODO (rejestr, analiza ryzyka, umowy powierzenia).

c) wdrażania ocen skutków dla ochrony danych (DPIA), szczególnie tam, gdzie AI wpływa na decyzje wobec osób fizycznych. DPIA jest **obowiązkowa**, jeżeli aplikacja lub system:

- przetwarza dane biometryczne lub zdrowotne,
- dokonuje zautomatyzowanego profilowania użytkowników,
- wykorzystuje algorytmy do podejmowania decyzji (np. scoring kredytowy, rekomendacje leczenia),
- zbiera dane lokalizacyjne w czasie rzeczywistym lub analizuje wzorce zachowań.

Wnioski: technologia nie zwalnia z obowiązków – wręcz przeciwnie

Im bardziej zaawansowana aplikacja lub system AI, tym większa odpowiedzialność za ochronę prywatności użytkownika. Ochrona danych osobowych musi być **nie tylko częścią specyfikacji projektu**, ale również jego trwałym elementem – aktualizowanym, testowanym i raportowanym.

6. Rosnąca odpowiedzialność działów sprzedaży i marketingu

W ostatnich latach działania marketingowe i sprzedażowe znalazły się w centrum zainteresowania organów ochrony danych. Dlaczego? Bo to właśnie w tym obszarze najłatwiej o naruszenia RODO i nowych przepisów krajowych – szczególnie w kontekście **marketingu bezpośredniego**, prowadzonego przez e-mail, telefon, SMS lub media społecznościowe.

Cold campaigns a dane osobowe – ryzyko „z automatu”

Coraz więcej firm prowadzi tzw. **cold campaigns**, czyli działania prospectingowe wobec osób, z którymi nie mieli wcześniej relacji (np. wysyłka e-maili do potencjalnych klientów, którzy nie zostawili swoich danych na stronie i nie wyrazili zgody). Tego typu działania są szczególnie ryzykowne z perspektywy RODO i **nowego Prawa komunikacji elektronicznej (PKE)**.

Wbrew powszechnemu przekonaniu, **nawet w relacjach B2B obowiązuje RODO**, jeśli dane identyfikują konkretną osobę (np. imię, nazwisko, służbowy e-mail: jan.kowalski@firma.pl). Firmy nie mogą zakładać, że kontakt „do firmy” wyłącza stosowanie przepisów – **jeśli komunikat dociera do osoby fizycznej, to podlega ochronie**.

Kluczowa zasada i najczęstsze błędy:

- **Jedna zgoda na wszystko -** zgoda musi być udzielona osobno dla każdego kanału kontaktu – np. e-mail, telefon, SMS. Nie można domniemywać, że zgoda na newsletter oznacza zgodę na cold call lub kampanię SMS.
- **„Zostawił wizytówkę, więc mogę dzwonić”** - nieprawda. Zostawienie wizytówki (np. na targach) uprawnia co najwyżej do jednorazowego, neutralnego kontaktu (np. z

podziękowaniem i pytaniem o zainteresowanie ofertą). Nie można na tej podstawie prowadzić cyklicznego marketingu czy kampanii automatycznych bez wyraźnej zgody.
- **Zgody domyślne lub ukryte** - zgody muszą być wyraźne, świadome, dobrowolne i jednoznaczne. Nie można ich „przemycać" w regulaminie ani domniemywać na podstawie braku sprzeciwu.

Podsumowanie: Compliance to nie wszystko – czas na „data accountability"

Organizacje coraz częściej rozumieją, że ochrona danych osobowych to nie tylko zgodność z przepisami, ale też budowanie zaufania, transparentności i przewidywalności. W erze cyfrowej to właśnie dane stanowią największe ryzyko... i największy kapitał.

Wniosek?
Zadbaj nie tylko o procedury, ale o ich realne zrozumienie i wdrożenie – na poziomie operacyjnym i technologicznym. Świadome zarządzanie danymi osobowymi staje się dziś jednym z filarów nowoczesnego, odpowiedzialnego biznesu.

Paweł Wojciechowski – adwokat, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.