

praktyczny przewodnik
prawny po ochronie

DANYCH OSOBOWYCH

w firmie



BY PISMO W SPRAWIE

**PRAKTYCZNY PRZEWODNIK PRAWNY
PO OCHRONIE DANYCH OSOBOWYCH
W FIRMIE**

Karolina Zuzanna Zdrojek

E-book prawny dla przedsiębiorców, osób zarządzających i praktyków.

Stan prawny: październik 2026 r.

Copyright © 2026 Karolina Zuzanna Zdrojek

ORCID: 0009-0003-1643-9288

Wydawca: (*self-publishing*) Pismo w Sprawie Karolina Zdrojek

Wszelkie prawa zastrzeżone.

Publikacja ma charakter edukacyjny.

Od Autorki

Ten e-book (tzw. e-książka) został stworzony jako praktyczne opracowanie prawne. Jego celem jest pokazanie, jak czytać i stosować przepisy o ochronie danych osobowych w realnych procesach firmy. Nie jest instrukcją konfiguracji systemów informatycznych ani podręcznikiem cyberbezpieczeństwa. Kwestie techniczne pojawiają się wyłącznie w takim zakresie, w jakim są potrzebne do wyjaśnienia obowiązków prawnych administratora lub podmiotu przetwarzającego.

Ochrona danych osobowych jest obszarem silnie zależnym od stanu faktycznego. Dlatego przykłady zawarte w niniejszej e-książce pokazują sposób kwalifikacji problemu, a nie zastępują analizy konkretnej sprawy. W miejscach, w których RODO pozostawia administratorowi ocenę ryzyka lub proporcjonalności, tekst wyraźnie wskazuje tę konieczność zamiast przedstawiać jedną odpowiedź jako automatyczną.

Fundamentalnym źródłem jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 o ochronie danych osobowych, zwany dalej skrótowo „RODO”. W zakresie polskiego porządku prawnego uwzględniono w szczególności ustawę z 10 maja 2018 r. o ochronie danych osobowych, Kodeks pracy oraz ustawę z 12 lipca 2024 r. Prawo komunikacji elektronicznej.

Gdybym miała zliczyć wszystkie błędne interpretacje RODO, zabrakłoby mi stron w tej e-książce. A przecież większości nieporozumień można byłoby uniknąć, po prostu czytając przepisy.

mgr Karolina Zuzanna Zdrojek

SPIS TREŚCI

1.	RODO od podstaw.	8
2.	Zanim zbierzesz dane, odpowiedz na pięć pytań.	11
3.	Zgoda nie jest lekarstwem na wszystko	13
4.	Dane wrażliwe. Tu zasady są inne.	16
5.	Klient wchodzi na Twoją stronę. Co dzieje się z jego danymi.	18
6.	Marketing zgodny z prawem.	22
7.	Obowiązek informacyjny bez ściany tekstu.	24
8.	Pracownicy, kandydaci i współpracownicy.	26
9.	Twoje dane są również u innych firm.	28
10.	Jak długo można przechowywać dane.	31
11.	Dokumentacja RODO, która rzeczywiście ma sens.	33
12.	Klient mówi: „usuńcie moje dane”.	36
13.	Wyciek danych. Pierwsze 72 godziny.	39
14.	Bezpieczeństwo danych bez budowania bunkra.	43
15.	AI w firmie a dane osobowe.	45

16.	Czy potrzebujesz IOD (inspektor ochrony danych osobowych) i DPIA (Data Protection Impact Assessment).....	48
17.	Kontrola UODO i odpowiedzialność.....	50
18.	Audyt RODO własnej firmy w jeden dzień.	52
19.	25 błędów RODO, które możesz znaleźć we własnej firmie.....	55
20.	RODO w praktyce. Plan naprawczy.	57
	CHECKLISTY	60
	Podstawy prawne i źródła	65

RODO jest prawem procesu.

RODO bywa przedstawiane jako zbiór formularzy: zgoda, klauzula informacyjna, polityka prywatności, rejestr i umowa powierzenia. Taki obraz jest wygodny, ale prawnie niepełny. Rozporządzenie konstruuje system odpowiedzialności administratora. To administrator ma znać cele przetwarzania, dobrać podstawy prawne, ograniczyć zakres danych, określić retencję, zapewnić realizację praw osób i umieć wykazać zgodność.

Najważniejszą zasadą tej książki jest rozdzielenie trzech pytań. Po pierwsze, co rzeczywiście dzieje się z danymi. Po drugie, jaka norma prawna znajduje zastosowanie. Po trzecie, jakie działania pozwalają wykazać zgodność. Dopiero po przejściu tych etapów dokument ma sens. Dokumentacja nie może tworzyć fikcyjnego świata równoległego do praktyki firmy.

RODO jest rozporządzeniem opartym na ryzyku. Nie oznacza to dowolności. Oznacza konieczność uzasadnienia decyzji. Administrator powinien potrafić odpowiedzieć nie tylko „co zrobiliśmy”, lecz również „dlaczego uznaliśmy to za zgodne z prawem”. Właśnie temu ma służyć dalsza część książki.

1. RODO od podstaw.

Punktem wyjścia jest art. 4 RODO, który definiuje między innymi dane osobowe, przetwarzanie, administratora i podmiot przetwarzający. Zakres zastosowania rozporządzenia wynika z art. 2 i 3 RODO. W praktyce prawnej pierwszym błędem bywa próba stosowania obowiązków RODO bez wcześniejszego ustalenia, czy konkretna informacja pozwala zidentyfikować osobę fizyczną oraz jaka rola przypada podmiotowi w danym procesie.

Zanim wybierzesz podstawę prawną, musisz znać operację przetwarzania.

Przetwarzaniem jest znacznie więcej niż zapisanie danych w bazie. Obejmuje między innymi zbieranie, utrwalanie, porządkowanie, przechowywanie, przeglądanie, wykorzystywanie, przesyłanie, udostępnianie, łączenie, ograniczanie i usuwanie danych. Dlatego firma, która twierdzi, że „nie przetwarza danych”, bo nie prowadzi rozbudowanego CRM, zazwyczaj i tak przetwarza dane klientów, pracowników, kontrahentów i osób kontaktujących się przez stronę.

Pierwszym zadaniem jest stworzenie mapy danych. Nie zaczynaj od nazw systemów. Zacznij od zdarzeń biznesowych: klient wysyła formularz, składa zamówienie, zapisuje się na wizytę, wystawia opinię, składa reklamację, wysyła CV, zapisuje się na newsletter. Do każdego zdarzenia przypisz dane, cel, podstawę, odbiorców, system, okres retencji i osobę odpowiedzialną.

Taka mapa pozwala wykryć procesy, których nie ma w polityce prywatności. Często są to arkusze handlowców, skrzynki pocztowe, komunikatory, formularze reklamowe, kopie zapasowe, systemy rezerwacji i narzędzia chmurowe.

Wypisz 10 najczęstszych zdarzeń, w których firma otrzymuje dane.

Dodaj systemy i dostawców używanych w każdym zdarzeniu.

Zaznacz procesy zawierające dane zdrowotne, biometryczne lub inne dane z art. 9 RODO.

Jeżeli informacja pozwala zidentyfikować osobę bezpośrednio albo pośrednio, może być daną osobową.

Imię i nazwisko są oczywistym przykładem, ale w praktyce równie ważne są adres e-mail, numer telefonu, identyfikator klienta, adres IP, identyfikator urządzenia, nagranie głosu, wizerunek, lokalizacja czy zestaw informacji pozwalających rozpoznać konkretną osobę. To, czy informacja jest daną osobową, zależy od kontekstu i realnych możliwości identyfikacji.

Błąd pojawia się, gdy firma uznaje dane za „anonimowe”, choć zachowuje klucz lub inne informacje pozwalające odtworzyć tożsamość. Pseudonimizacja może istotnie zmniejszać ryzyko, ale nie jest tym samym co anonimizacja. Dane pseudonimizowane nadal mogą podlegać RODO.

W praktyce warto oznaczyć kategorie danych nie tylko według nazwy pola w systemie, lecz według ryzyka. Inaczej traktuje się sam adres e-mail do newslettera, inaczej kopię dokumentu tożsamości, a jeszcze inaczej dokumentację zdrowotną. Im bardziej dotkliwe mogą być skutki utraty poufności, tym mocniejsze zabezpieczenia i bardziej świadome decyzje są potrzebne.

Czy wiesz, które identyfikatory techniczne zapisuje Twoja strona?

Czy „anonimowe” zestawy da się połączyć z innymi danymi?

Czy klasyfikujesz dane według wrażliwości i skutków naruszenia?

Nie każda firma, która dostaje dane od Ciebie, jest podmiotem przetwarzającym.

Administrator ustala cele i sposoby przetwarzania. Procesor przetwarza dane w imieniu administratora i na jego udokumentowane polecenie. To rozróżnienie ma praktyczne konsekwencje. Jeżeli dostawca działa we własnym celu i samodzielnie określa istotne elementy przetwarzania, nie wystarczy nazwać go procesorem w umowie.

Przykładowo dostawca hostingu lub systemu rezerwacji może działać jako procesor w zakresie danych przechowywanych na rzecz klienta. Inny odbiorca może być odrębnym administratorem, jeżeli otrzymuje dane na własnej podstawie i realizuje własne obowiązki. Możliwe jest też współadministrowanie, gdy dwa podmioty wspólnie ustalają cele i sposoby określonego procesu.

Zanim podpiszesz umowę powierzenia, opisz faktyczny przepływ danych. Zapytaj kto decyduje po co dane są używane, kto ustala okres przechowywania, kto odpowiada na żądania osób i czy dostawca może wykorzystywać dane do własnych celów.

Zrób listę wszystkich dostawców mających dostęp do danych.

Przypisz każdemu rolę: procesor, odrębny administrator, współadministrator lub brak dostępu do danych.

Jak przeprowadzić kwalifikację prawną

- Czy informacja dotyczy zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej?
- Jaką rolę pełni podmiot w tym konkretnym procesie?
- Czy RODO ma zastosowanie terytorialne i materialne?

2. Zanim zbierzesz dane, odpowiedz na pięć pytań.

Każdy proces powinien być oceniany przez pryzmat zasad z art. 5 ust. 1 RODO oraz zasady rozliczalności z art. 5 ust. 2. Legalność nie sprowadza się do wskazania podstawy z art. 6. Administrator powinien umieć wykazać cel, adekwatny zakres danych, okres retencji, krąg odbiorców oraz sposób realizacji praw osoby.

Jeżeli nie wiesz, od czego zacząć analizę, wróć do art. 5 RODO.

Zasady z art. 5 RODO są szkieletem całego systemu. Dane mają być przetwarzane zgodnie z prawem, rzetelnie i przejrzysto. Mają być zbierane w konkretnych i prawnie uzasadnionych celach. Zakres danych ma być ograniczony do tego, co potrzebne. Dane powinny być prawidłowe. Nie wolno przechowywać ich dłużej niż wymaga tego cel. Trzeba zapewnić odpowiednie bezpieczeństwo.

Osobną rolę pełni rozliczalność. Administrator nie tylko ma przestrzegać zasad, lecz także powinien być w stanie to wykazać. W praktyce oznacza to decyzje udokumentowane w sposób proporcjonalny do ryzyka: rejestry, procedury, analizy, konfiguracje systemów, szkolenia, umowy, logi i dowody realizacji żądań.

Art. 5 jest też dobrym testem dla nowych pomysłów biznesowych. Jeśli zespół chce zbierać dodatkowe dane „bo mogą się kiedyś przydać”, pojawia się pytanie o cel i minimalizację. Jeśli baza ma być przechowywana bezterminowo, pojawia się ograniczenie przechowywania. Jeśli klient nie rozumie procesu, pojawia się przejrzystość.

Czy potrafisz wykazać decyzje dotyczące ryzyka i bezpieczeństwa?

Danych, których nie zbierzesz, nie musisz później chronić, aktualizować ani usuwać.

Minimalizacja wymaga, aby zakres danych był adekwatny, stosowny i ograniczony do tego, co niezbędne. Każde pole formularza powinno mieć uzasadnienie. Jeżeli do wysyłki newslettera wystarcza adres e-mail, żądanie daty urodzenia i adresu zamieszkania wymaga dodatkowego celu i podstawy.

W praktyce minimalizacja dotyczy też dostępu. To, że firma legalnie posiada dane, nie oznacza, że każdy pracownik powinien je widzieć. Role i uprawnienia powinny odpowiadać obowiązkom. Handlowiec nie musi mieć dostępu do pełnej dokumentacji kadrowej, a osoba obsługująca płatności nie zawsze potrzebuje treści korespondencji klienta.

Minimalizacja obniża koszty incydentu. Im mniejszy zakres danych i liczba osób z dostępem, tym mniejsza powierzchnia ryzyka. Jest to więc jednocześnie zasada prawna i praktyka bezpieczeństwa.

Usuń pola formularzy, których celu nie potrafisz wyjaśnić.

Przejrzyj uprawnienia użytkowników w systemach.

Ogranicz eksporty danych do arkuszy i lokalnych plików.

Jak przeprowadzić kwalifikację prawną

- Jaki jest konkretny cel przetwarzania?
- Czy zakres danych jest niezbędny do tego celu?
- Jak administrator wykaże zgodność z art. 5 ust. 2 RODO?

3. Zgoda nie jest lekarstwem na wszystko

Podstawy legalności przetwarzania określa art. 6 ust. 1 RODO. Zgoda z art. 6 ust. 1 lit. a jest tylko jedną z nich. Warunki skutecznej zgody wynikają przede wszystkim z art. 4 pkt 11 i art. 7 RODO. Jeżeli przetwarzanie jest konieczne do wykonania umowy, wypełnienia obowiązku prawnego albo może opierać się na prawnie uzasadnionym interesie, mechaniczne odbieranie zgody może prowadzić do błędnej kwalifikacji prawnej.

Zgoda jest jedną z podstaw, a nie domyślnym rozwiązaniem.

Art. 6 ust. 1 RODO przewiduje kilka podstaw przetwarzania. W relacji z klientem często kluczowe są działania przed zawarciem umowy i wykonanie umowy. Inne procesy wynikają z obowiązku prawnego. Część może opierać się na prawnie uzasadnionym interesie administratora lub strony trzeciej, o ile nie przeważają interesy, prawa i wolności osoby.

Zgoda ma sens wtedy, gdy osoba rzeczywiście ma wybór i może ją wycofać bez negatywnych konsekwencji. Jeśli usługa obiektywnie wymaga określonych danych, zwykle nie ma potrzeby tworzenia fikcyjnej zgody na ich użycie do wykonania umowy. Zła podstawa prawna prowadzi potem do błędnych komunikatów, problemów z wycofaniem zgody i nieprawidłowych okresów retencji.

Dla każdego celu wybierz podstawę oddzielnie. Ten sam adres e-mail może być przetwarzany w celu realizacji zamówienia, obsługi reklamacji, zabezpieczenia roszczeń i marketingu. To nie jest jeden proces tylko dlatego, że pole danych jest to samo.

Dla każdego celu wskaż jedną główną podstawę z art. 6 ust. 1 RODO.

Nie kopiuj podstaw z cudzej polityki prywatności.

Oddziel wykonanie umowy od marketingu i innych celów pobocznych.

Dobra zgoda daje wybór, zła zgoda maskuje brak analizy.

Zgoda powinna być dobrowolna, konkretna, świadoma i jednoznaczna. Administrator musi móc wykazać jej uzyskanie. Jeśli oświadczenie o zgodzie jest częścią szerszego dokumentu, powinno być odróżnialne od innych kwestii i napisane jasnym językiem.

W praktyce nie łącz w jednym checkboxie kilku niezależnych celów. Zgoda na newsletter nie powinna automatycznie obejmować publikacji wizerunku, kontaktu telefonicznego i przekazywania danych partnerom. Jeżeli cele są rozdzielne, osoba powinna móc dokonać rozdzielnych wyborów.

Równie ważne jest wycofanie zgody. RODO wymaga, aby było równie łatwe jak jej wyrażenie. System powinien zapisywać fakt wycofania i zatrzymywać procesy oparte na zgodzie, ale nie oznacza to automatycznego usunięcia wszystkich danych. Inna część danych może nadal być potrzebna na innej podstawie, na przykład do rozliczeń lub obrony roszczeń.

Czy zapisujesz, kiedy, jak i na jaką treść osoba wyraziła zgodę?

Czy wycofanie zgody uruchamia realny proces w systemach?

Art. 6 ust. 1 lit. f RODO nie oznacza „firma ma interes, więc może”.

Prawnie uzasadniony interes wymaga analizy. Najpierw określ interes administratora lub strony trzeciej. Następnie sprawdź, czy przetwarzanie jest rzeczywiście potrzebne do jego realizacji.

Na końcu zważ ten interes z prawami, wolnościami i rozsądnymi oczekiwaniami osoby.

Dobra analiza opisuje konkretny proces, zakres danych, relację z osobą, potencjalne korzyści i szkody, zabezpieczenia oraz możliwość sprzeciwu. Nie musi być wielostronicowym memorandum w każdej prostej sprawie, ale powinna pozwolić wykazać, dlaczego firma uznała daną operację za dopuszczalną.

W praktyce interes może być rozważany między innymi przy bezpieczeństwie systemów, zapobieganiu nadużyciom, części działań analitycznych czy dochodzeniu i obronie roszczeń. Każdy przypadek wymaga jednak oceny kontekstu. Szczególną ostrożność trzeba zachować wobec dzieci i przy procesach, których osoba nie może rozsądnie oczekiwać.

Wyjaśnij, dlaczego celu nie da się osiągnąć mniej ingerującym sposobem.

Zapisz zabezpieczenia ograniczające wpływ na osobę.

Jak przeprowadzić kwalifikację prawną

- Która przesłanka z art. 6 ust. 1 rzeczywiście odpowiada celowi?
- Czy zgoda jest dobrowolna i możliwa do wycofania bez negatywnych konsekwencji?
- Czy przy art. 6 ust. 1 lit. f przeprowadzono test równowagi?

4. Dane wrażliwe. Tu zasady są inne.

Szczególne kategorie danych zostały wskazane w art. 9 ust. 1 RODO. Ich przetwarzanie jest co do zasady zabronione, chyba że zachodzi jedna z przesłanek z art. 9 ust. 2. Dane dotyczące wyroków skazujących i czynów zabronionych podlegają odrębnemu reżimowi art. 10 RODO. W tych obszarach sama przesłanka z art. 6 może nie wystarczyć.

Dane o zdrowiu wymagają nie tylko podstawy z art. 6, lecz także spełnienia warunku z art. 9 RODO.

Do szczególnych kategorii należą między innymi dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, przynależność do związków zawodowych, dane genetyczne, określone dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Co do zasady ich przetwarzanie jest zabronione, chyba że zachodzi wyjątek przewidziany w art. 9 ust. 2 RODO.

W branży medycznej, beauty, dietetycznej i wellness granica bywa przekraczana bardzo szybko. Informacja o alergii, ciąży, lekach, chorobie przewlekłej czy przeciwwskazaniach jest informacją o zdrowiu. Formularz, który z pozoru służy „lepszemu dopasowaniu usługi”, może więc wejść w reżim art. 9.

Nie zbieraj danych zdrowotnych „na wszelki wypadek”. Ustal, czy są konieczne, jaka przesłanka z art. 9 ust. 2 ma zastosowanie, kto ma dostęp i jak długo dane są potrzebne. Wysoka wrażliwość danych powinna wpływać także na środki bezpieczeństwa i ocenę ryzyka.

Zidentyfikuj wszystkie pola formularzy dotyczące zdrowia.

Ogranicz dostęp do osób, które rzeczywiście go potrzebują.

Jak przeprowadzić kwalifikację prawną

- Czy dane należą do art. 9 ust. 1 lub art. 10 RODO?
- Jaka przesłanka szczególna legalizuje przetwarzanie?
- Czy zakres i zabezpieczenia odpowiadają podwyższonemu ryzyku?

5. Klient wchodzi na Twoją stronę. Co dzieje się z jego danymi.

Strona internetowa może uruchamiać kilka odrębnych procesów prawnych. Formularz kontaktowy, konto użytkownika, newsletter, narzędzia analityczne i mechanizmy przechowywania informacji w urzędzeniu końcowym nie powinny być traktowane jako jeden proces. Dla każdego należy oddzielnie ustalić cel, podstawę, obowiązek informacyjny, odbiorców oraz retencję.

Klauzula informacyjna ma wyjaśniać proces, a nie odstraszać długością.

Gdy dane są zbierane od osoby, podstawowy zakres informacji wynika z art. 13 RODO. Gdy pochodzą z innego źródła, znaczenie ma art. 14 RODO. Osoba powinna wiedzieć między innymi kto jest administratorem, w jakich celach i na jakich podstawach dane są przetwarzane, komu mogą być ujawniane, jak długo będą przechowywane i jakie prawa jej przysługują.

Nie wystarczy umieścić w stopce strony ogólnego linku do dokumentu, który nie odpowiada konkretnemu procesowi. Informacja ma być przekazana w sposób przejrzysty i łatwo dostępny. W rozbudowanych usługach można stosować warstwowe podejście: najważniejsze informacje podać bezpośrednio, a szczegóły udostępnić w pełnej polityce.

Klauzula powinna być aktualizowana wraz z procesem. Jeżeli firma wdraża nowy system, dodaje odbiorców, zmienia cele lub zaczyna transferować dane poza EOG, dokumentacja i komunikacja z osobami powinny zostać zweryfikowane.

Czy klauzula wskazuje realne cele, a nie ogólne hasła?

Czy okresy przechowywania są konkretne albo możliwe do ustalenia?

Czy informacja jest dostępna w momencie zbierania danych?

Najgorsza polityka prywatności to taka, która wygląda profesjonalnie, ale opisuje inną firmę.

Kopowanie dokumentu od konkurencji jest ryzykowne, ponieważ każda organizacja korzysta z innych systemów, dostawców, kanałów marketingowych i okresów retencji. Dokument powinien być rezultatem mapy procesów, a nie jej substytutem.

Przejrzyj politykę zdanie po zdaniu i sprawdź, czy potrafisz wskazać dowód na każde twierdzenie. Jeśli piszesz, że dane nie są przekazywane poza EOG, sprawdź dostawców chmury, analityki, reklam i komunikacji. Jeśli deklarujesz usuwanie danych po określonym czasie, sprawdź, czy istnieje mechanizm usuwania także z archiwów i systemów pomocniczych.

Dobra polityka nie musi być przesadnie długa. Powinna być prawdziwa, zrozumiała i powiązana z realnymi procesami. Jeżeli firma ma kilka wyraźnie różnych grup osób, można rozważyć odrębne klauzule dla klientów, kandydatów do pracy, kontrahentów czy użytkowników strony.

Porównaj politykę z listą faktycznych dostawców.

Sprawdź, czy wymienione prawa mają procedurę obsługi.

Zweryfikuj, czy deklarowane terminy retencji są technicznie realizowane.

Prawo komunikacji elektronicznej reguluje także przechowywanie informacji lub uzyskiwanie dostępu do informacji już przechowywanej w urządzeniu końcowym użytkownika. W praktyce

dotyczy to między innymi mechanizmów cookies i podobnych technologii.

Baner powinien odpowiadać rzeczywistej konfiguracji strony. Jeżeli narzędzia analityczne lub reklamowe uruchamiają się przed dokonaniem wyboru przez użytkownika, mimo że wymagają zgody, estetyczny panel nie naprawia problemu. Trzeba sprawdzić zachowanie strony technicznie.

Warto prowadzić inwentaryzację technologii śledzących, ich dostawców, celów, czasu działania i przepływów danych. Po każdej większej zmianie strony lub dodaniu wtyczki warto ponowić test. Ochrona danych w fazie projektowania oznacza, że prywatność powinna być uwzględniana już przy wdrożeniu funkcji, a nie po publikacji serwisu.

Powiąz opis cookies z rzeczywistymi dostawcami.

Prosty formularz potrafi uruchomić kilka różnych procesów.

Jeżeli osoba wysyła zapytanie o usługę, przetwarzanie może być związane z podjęciem działań na jej żądanie przed zawarciem umowy. Nie oznacza to jednak, że dane z zapytania można bez dodatkowej analizy przenieść do każdej kampanii marketingowej.

Formularz powinien zbierać tylko dane potrzebne do odpowiedzi. Pole „wiadomość” jest szczególnie ryzykowne, bo użytkownicy mogą wpisywać tam dane, których firma nie potrzebuje, w tym informacje o zdrowiu lub sytuacji osobistej. Warto ograniczyć instrukcją zakres treści i odpowiednio zabezpieczyć skrzynkę odbiorczą.

Po zakończeniu kontaktu trzeba zdecydować, jak długo lead będzie przechowywany. Inaczej może wyglądać retencja zwykłego pytania, inaczej negocjacji, z których mogą powstać roszczenia. Okres

powinien wynikać z celu, ryzyka i właściwych przepisów, a nie z domyślnego „na zawsze”.

Nie dodawaj leadów automatycznie do newslettera bez właściwej podstawy i spełnienia wymagań kanału.

Jak przeprowadzić kwalifikację prawną

- Jakie odrębne procesy uruchamia strona?
- Czy użytkownik otrzymuje właściwą informację przed lub przy pozyskaniu danych?
- Czy mechanizmy na urządzeniu końcowym spełniają wymogi PKE?

6. Marketing zgodny z prawem.

Marketing elektroniczny wymaga łącznej analizy RODO oraz ustawy z 12 lipca 2024 r. Prawo komunikacji elektronicznej. Art. 398 PKE ustanawia reguły używania automatycznych systemów wywołujących oraz telekomunikacyjnych urządzeń końcowych do przesyłania informacji handlowej, w tym marketingu bezpośredniego. Podstawa przetwarzania danych na gruncie RODO i wymóg wynikający z PKE to dwa odrębne poziomy oceny.

Legalne posiadanie adresu e-mail nie oznacza automatycznie prawa do wysyłania reklamy.

Przy marketingu trzeba oddzielić podstawę przetwarzania danych od zasad korzystania z kanału komunikacji. Od 10 listopada 2024 r. kluczowe znaczenie ma art. 398 Prawa komunikacji elektronicznej. Przepis reguluje używanie automatycznych systemów wywołujących i telekomunikacyjnych urządzeń końcowych do przesyłania informacji handlowej, w tym marketingu bezpośredniego.

Dlatego analiza powinna mieć co najmniej dwa poziomy. Pierwszy: czy firma może przetwarzać dane dla określonego celu na gruncie RODO. Drugi: czy może wykorzystać konkretny kanał, na przykład e-mail, SMS lub telefon, zgodnie z PKE. Nie wolno mieszać tych pytań w jednym ogólnym checkboxie.

Zgody marketingowe powinny być udokumentowane. System musi też respektować ich wycofanie i sprzeciw wobec marketingu bezpośredniego. Lista blokująca może być potrzebna właśnie po to, aby nie skontaktować się ponownie z osobą, która sprzeciwiła się marketingowi.

Synchronizuj wypisanie z newslettera z systemami marketingowymi.

Jak przeprowadzić kwalifikację prawną

- Czy istnieje podstawa przetwarzania danych na gruncie RODO?
- Czy kanał komunikacji wymaga uprzedniej zgody na gruncie PKE?
- Czy sprzeciw lub wycofanie zgody jest skutecznie respektowane?

7. Obowiązek informacyjny bez ściany tekstu.

Zakres obowiązku informacyjnego zależy od źródła danych. Art. 13 RODO dotyczy danych zbieranych od osoby, a art. 14 danych pozyskanych z innego źródła. Informacja ma być przekazana w sposób zwięzły, przejrzysty, zrozumiały i łatwo dostępny zgodnie z art. 12 RODO. Nie jest prawidłową praktyką zastępowanie obowiązku informacyjnego samym linkiem do ogólnej polityki, jeżeli nie pozwala on osobie zrozumieć konkretnego procesu.

Klauzula informacyjna ma wyjaśniać proces, a nie odstraszać długością.

Gdy dane są zbierane od osoby, podstawowy zakres informacji wynika z art. 13 RODO. Gdy pochodzą z innego źródła, znaczenie ma art. 14 RODO. Osoba powinna wiedzieć między innymi kto jest administratorem, w jakich celach i na jakich podstawach dane są przetwarzane, komu mogą być ujawniane, jak długo będą przechowywane i jakie prawa jej przysługują.

Nie wystarczy umieścić w stopce strony ogólnego linku do dokumentu, który nie odpowiada konkretnemu procesowi. Informacja ma być przekazana w sposób przejrzysty i łatwo dostępny. W rozbudowanych usługach można stosować warstwowe podejście: najważniejsze informacje podać bezpośrednio, a szczegóły udostępnić w pełnej polityce.

Klauzula powinna być aktualizowana wraz z procesem. Jeżeli firma wdraża nowy system, dodaje odbiorców, zmienia cele lub zaczyna transferować dane poza EOG, dokumentacja i komunikacja z osobami powinny zostać zweryfikowane.

Czy klauzula wskazuje realne cele, a nie ogólne hasła?

Czy okresy przechowywania są konkretne albo możliwe do ustalenia?

Czy informacja jest dostępna w momencie zbierania danych?

Jak przeprowadzić kwalifikację prawną

- Czy zastosowanie ma art. 13 czy 14 RODO?
- Czy komunikat obejmuje wszystkie wymagane elementy?
- Czy język odpowiada zasadom art. 12 RODO?

8. Pracownicy, kandydaci i współpracownicy.

W relacjach pracowniczych RODO działa łącznie z Kodeksem pracy. Zakres danych żądanych od kandydata i pracownika określa w szczególności art. 22(1) Kodeksu pracy, a reguły dotyczące zgody i danych szczególnych kategorii uzupełniają art. 22(1a) i 22(1b). Monitoring pracowniczy podlega odrębnym warunkom z art. 22(2) i 22(3) Kodeksu pracy.

CV nie jest zgodą na dowolne wykorzystanie danych kandydata.

Proces rekrutacyjny wymaga uwzględnienia przepisów prawa pracy oraz RODO. Zakres danych, których pracodawca może żądać, nie jest dowolny. Jeżeli kandydat przekazuje dodatkowe informacje z własnej inicjatywy, trzeba ocenić podstawę i cel ich dalszego przetwarzania.

Osobno należy potraktować obecną rekrutację i ewentualne przyszłe rekrutacje. To, że CV trafiło do firmy w odpowiedzi na konkretne ogłoszenie, nie oznacza automatycznie możliwości przechowywania go bezterminowo na potrzeby wszystkich przyszłych naborów.

Szczególną ostrożność zachowaj wobec danych szczególnych kategorii oraz informacji, których pracodawca nie powinien pozyskiwać. Ogranicz dostęp do dokumentów rekrutacyjnych, ustal retencję i usuń kopie z prywatnych skrzynek osób uczestniczących w procesie.

Oddziel rekrutację bieżącą od bazy przyszłych kandydatów.

Sprawdź zakres danych wymaganych w formularzu.

Ustal kto ma dostęp do CV i kiedy kopie są usuwane.

Dostęp do danych powinien wynikać z roli, nie z samego faktu pracy w firmie.

Organizacja powinna wiedzieć kto ma dostęp do jakich kategorii danych i dlaczego. Upoważnienia, role systemowe i zasada najmniejszych uprawnień pomagają ograniczyć ryzyko zarówno przypadkowego błędu, jak i nadużycia.

Pracownik powinien otrzymać praktyczne instrukcje: jak wysłać korespondencję do wielu osób, jak weryfikować odbiorcę, gdzie zapisywać pliki, jak zgłaszać incydenty, czy wolno używać prywatnych komunikatorów i urządzeń, jak postępować z wydrukami oraz kiedy blokować ekran. Sam podpis pod ogólną polityką bezpieczeństwa nie wystarczy, jeśli procedura nie przekłada się na zachowanie.

Po zmianie stanowiska lub zakończeniu współpracy uprawnienia powinny być niezwłocznie zmienione lub odebrane. Konta nieużywane przez byłych pracowników są prostym przykładem ryzyka, które można ograniczyć organizacyjnie.

Odbieraj uprawnienia po zmianie roli i odejściu.

Szkolenia opieraj na realnych incydentach i systemach używanych w firmie.

Jak przeprowadzić kwalifikację prawną

- Czy żądane dane mieszczą się w Kodeksie pracy?
- Czy dodatkowe dane są rzeczywiście dobrowolne?
- Czy monitoring ma ustawową podstawę, cel i prawidłową informację?

9. Twoje dane są również u innych firm.

Powierzenie przetwarzania podlega art. 28 RODO. Sam fakt korzystania z zewnętrznej firmy nie przesądza jednak, że mamy do czynienia z procesorem. Konieczne jest ustalenie, kto określa cele i sposoby przetwarzania. Przy transferach poza EOG trzeba dodatkowo stosować rozdział V RODO, w szczególności art. 44 i następne.

Umowa powierzenia ma opisywać odpowiedzialny sposób wykonywania przetwarzania w imieniu administratora.

Art. 28 RODO określa elementy relacji administratora z procesorem. Umowa lub inny instrument prawny powinny między innymi określać przedmiot i czas trwania przetwarzania, jego charakter i cel, rodzaj danych, kategorie osób oraz prawa i obowiązki administratora.

Procesor powinien działać na udokumentowane polecenie, zapewnić poufność osób upoważnionych, stosować odpowiednie środki bezpieczeństwa, pomagać w realizacji praw osób i obowiązków dotyczących bezpieczeństwa, naruszeń oraz ocen skutków, a po zakończeniu usług usunąć lub zwrócić dane zgodnie z decyzją administratora, o ile prawo nie wymaga dalszego przechowywania.

Nie traktuj umowy powierzenia jak załącznika podpisywanego automatycznie. Sprawdź podprocesorów, lokalizacje danych, procedurę incydentów, możliwość audytu, sposób zwrotu danych i zasady zmian w łańcuchu dostawców.

Czy znasz podprocesorów i sposób informowania o zmianach?

Czy wiesz, jak odzyskać i usunąć dane po zakończeniu umowy?

Outsourcing usługi nie oznacza outsourcingu decyzji administratora.

Popularny system może mieć wysoki poziom bezpieczeństwa, ale administrator nadal powinien ocenić, czy sposób jego użycia odpowiada charakterowi danych i ryzyku. Istotne są konfiguracje kont, uwierzytelnianie, role, logi, kopie zapasowe, retencja, lokalizacja danych i podprocesory.

W umowach typu SaaS część warunków jest narzucona przez dostawcę. To nie zwalnia firmy z obowiązku przeczytania dokumentacji i podjęcia świadomej decyzji. Jeżeli dostawca nie daje informacji potrzebnych do oceny zgodności albo jego model wykorzystania danych jest sprzeczny z celem administratora, trzeba rozważyć inne rozwiązanie.

Najczęstszy problem nie wynika z samej chmury, lecz z konfiguracji. Publiczny link do dokumentu, brak MFA, konto współdzielone przez zespół czy nieograniczone eksporty mogą zniweczyć nawet dobre zabezpieczenia dostawcy.

Zakazuj współdzielonych kont, jeśli system pozwala na konta indywidualne.

„Serwer w Europie” nie zawsze kończy analizę transferu.

Przekazywanie danych do państw trzecich wymaga spełnienia warunków rozdziału V RODO. W zależności od państwa i dostawcy znaczenie może mieć decyzja stwierdzająca odpowiedni stopień ochrony albo odpowiednie zabezpieczenia, takie jak standardowe klauzule umowne, wraz z oceną warunków transferu, gdy jest potrzebna.

Analizuj nie tylko głównego dostawcę, ale także jego podprocesorów i dostęp administracyjny. Dokumentacja usługi powinna pozwalać ustalić, gdzie dane są przechowywane, skąd mogą być dostępne i jakie mechanizmy prawne są stosowane.

Polityka prywatności powinna uczciwie informować o transferach, jeżeli zachodzą. Nie wpisuj automatycznie, że dane „nie opuszczają EOG”, tylko dlatego, że wybrano europejski region centrum danych.

Ustal podstawę transferu dla każdego istotnego przepływu.

Zweryfikuj, czy informacje dla osób odpowiadają rzeczywistości.

Jak przeprowadzić kwalifikację prawną

- Czy kontrahent działa w imieniu administratora czy dla własnych celów?
- Czy umowa spełnia art. 28 ust. 3 RODO?
- Czy dochodzi do transferu do państwa trzeciego?

10. Jak długo można przechowywać dane.

Zasada ograniczenia przechowywania wynika z art. 5 ust. 1 lit. e RODO. Rozporządzenie nie ustanawia jednego terminu dla wszystkich danych. Okres przechowywania powinien wynikać z celu, obowiązków szczególnych oraz realnej potrzeby zabezpieczenia roszczeń. Administrator powinien potrafić uzasadnić przyjęty termin, a nie jedynie wpisać ogólną formułę „do czasu przedawnienia”.

Każda kategoria danych powinna mieć logiczny moment końcowy.

Zasada ograniczenia przechowywania wymaga, aby dane były przechowywane nie dłużej, niż jest to niezbędne do celów. Nie zawsze da się wskazać jedną datę dla całej bazy. Różne dokumenty mogą podlegać różnym obowiązkom ustawowym i różnym ryzykom roszczeń.

Najlepszym narzędziem jest harmonogram retencji. Dla każdej kategorii danych określ zdarzenie rozpoczynające bieg okresu, długość okresu, podstawę decyzji, systemy objęte usuwaniem i ewentualne wyjątki. Uwzględnij także kopie robocze, skrzynki pocztowe i eksporty.

Usunięcie nie zawsze musi oznaczać natychmiastowe fizyczne wymazanie każdej kopii zapasowej, jeśli backup działa w kontrolowanym cyklu i dane nie są używane operacyjnie. Ważne jest jednak, aby proces był zaprojektowany, udokumentowany i zgodny z celem.

Stwórz tabelę retencji dla głównych procesów.

Zdefiniuj zdarzenie startowe dla każdego terminu.

Sprawdź, czy system technicznie potrafi wykonać usunięcie.

Jak przeprowadzić kwalifikację prawną

- Z jakiego celu wynika okres przechowywania?
- Czy szczególny przepis wymaga przechowania danych?
- Czy po ustaniu celu dane są usuwane, anonimizowane lub ograniczane?

11. Dokumentacja RODO, która rzeczywiście ma sens.

RODO opiera się na rozliczalności. Dokumentacja ma umożliwiać wykazanie zgodności, a nie tylko istnieć. Rejestr czynności przetwarzania reguluje art. 30 RODO. Dokumentowanie naruszeń wynika z art. 33 ust. 5. Ocena skutków z art. 35 jest wymagana w przypadkach wysokiego ryzyka. Zakres dokumentacji powinien odpowiadać rzeczywistym procesom i ryzyku.

Rejestr ma być mapą odpowiedzialności, a nie tabelą stworzoną tylko na kontrolę.

Art. 30 RODO określa obowiązki dotyczące rejestrowania czynności przetwarzania. Wyjątek dla podmiotów zatrudniających mniej niż 250 osób jest ograniczony. Nie działa między innymi wtedy, gdy przetwarzanie nie ma charakteru sporadycznego, może powodować ryzyko lub obejmuje dane szczególnych kategorii albo dane dotyczące wyroków i czynów zabronionych.

Dla małej firmy wiele podstawowych procesów jest stałych, a nie sporadycznych: obsługa klientów, księgowość, zatrudnienie czy marketing. Dlatego założenie „mamy mniej niż 250 osób, więc rejestr nas nie dotyczy” może być błędne.

Dobry rejestr pomaga zarządzać retencją, odbiorcami, transferami i zabezpieczeniami. Powinien być aktualizowany przy zmianach procesu, a nie raz na kilka lat.

Porównaj rejestr z mapą systemów i dostawców.

Dodaj procesy powtarzalne, których wcześniej nie opisano.

Brak zgłoszenia do UODO nie oznacza braku dokumentacji zdarzenia.

Art. 33 ust. 5 RODO nakłada obowiązek dokumentowania naruszeń ochrony danych, obejmującego okoliczności naruszenia, jego skutki i podjęte działania zaradcze. Dokumentacja ma umożliwić organowi nadzorczemu weryfikację przestrzegania przepisu.

Rejestr naruszeń powinien zawierać co najmniej daty, opis zdarzenia, kategorie i zakres danych, liczbę osób w miarę możliwości, ocenę ryzyka, decyzję o zgłoszeniu lub braku zgłoszenia, informację o zawiadomieniu osób i działania naprawcze.

Dobrze prowadzony rejestr pokazuje też powtarzające się źródła błędów. Jeżeli co miesiąc występują pomyłki przy wysyłce, problem nie jest jednostkowy. To sygnał do zmiany procesu, narzędzia albo szkolenia.

Co kwartał analizuj powtarzające się przyczyny.

Najlepsze przygotowanie do kontroli to proces, który działa przed kontrolą.

Administrator powinien być w stanie wykazać zgodność. W praktyce oznacza to spójny zestaw dowodów: mapę procesów, rejestry, klauzule, podstawy prawne, testy równowagi, umowy z procesorami, analizy ryzyka, DPIA, gdy wymagane, procedury praw osób, rejestr naruszeń, dokumentację szkoleń i dowody przeglądów uprawnień.

Nie chodzi o liczbę dokumentów. Organ może pytać o to, jak procedura działa w praktyce. Jeżeli polityka przewiduje kwartalny przegląd uprawnień, a firma nigdy go nie wykonała, dokument może wręcz ujawnić rozbieżność.

Ważna jest też współpraca z organem. Art. 31 RODO nakłada obowiązek współpracy na administratora i procesora. Odpowiedzi powinny być kompletne, terminowe i oparte na faktach.

Nie twórz dokumentów, których firma nie zamierza stosować.

Wyznacz osobę koordynującą kontakt z organem.

Jak przeprowadzić kwalifikację prawną

- Czy dokumentacja odzwierciedla rzeczywiste procesy?
- Czy organizacja potrafi wykazać decyzje dotyczące podstaw, retencji i ryzyka?
- Czy dokumenty są aktualizowane po zmianach procesów?

12. Klient mówi: „usuńcie moje dane”.

Prawa osoby, której dane dotyczą, tworzą system określony przede wszystkim w art. 12–22 RODO. Żądanie usunięcia nie oznacza automatycznego obowiązku skasowania każdej informacji. Art. 17 przewiduje zarówno przesłanki usunięcia, jak i wyjątki. Każdy wniosek wymaga kwalifikacji prawnej oraz udokumentowania sposobu jego rozpoznania.

Wniosek klienta nie powinien uruchamiać paniki i ręcznego przeszukiwania całej firmy.

Art. 15 RODO daje osobie prawo uzyskania potwierdzenia, czy jej dane są przetwarzane, dostępu do danych oraz określonych informacji o przetwarzaniu. Osoba ma także prawo do kopii danych podlegających przetwarzaniu, z uwzględnieniem praw i wolności innych osób.

Procedura powinna określać kto przyjmuje wniosek, jak weryfikuje tożsamość, jakie systemy przeszukuje, kto zatwierdza odpowiedź i jak odnotowuje termin. Co do zasady administrator udziela informacji bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca. W określonych warunkach termin może zostać przedłużony, o czym trzeba poinformować osobę.

Nie utożsamiaj prawa dostępu z obowiązkiem wysłania wszystkich dokumentów firmowych bez analizy. Przed udostępnieniem trzeba uwzględnić dane innych osób, tajemnice i zakres samego prawa.

Prawo do bycia zapomnianym ma przesłanki i wyjątki.

Art. 17 RODO wskazuje sytuacje, w których osoba może żądać usunięcia danych, między innymi, gdy dane nie są już potrzebne,

zgoda została cofnięta i brak innej podstawy, osoba skutecznie wniosła sprzeciw albo dane były przetwarzane niezgodnie z prawem.

Jednocześnie prawo do usunięcia nie ma charakteru absolutnego. RODO przewiduje wyjątki, między innymi, gdy przetwarzanie jest niezbędne do wywiązania się z obowiązku prawnego albo do ustalenia, dochodzenia lub obrony roszczeń.

Dlatego odpowiedź „nie możemy usunąć, bo RODO” jest równie zła jak bezrefleksyjne skasowanie wszystkiego. Trzeba rozbić dane według celów i podstaw. Newsletter może zostać zatrzymany, a dokument księgowy nadal przechowywany przez okres wynikający z prawa.

Usuń to, czego nie ma podstawy dalej przechowywać.

Wyjaśnij osobie zakres odmowy i jej podstawę.

Nie wszystkie prawa działają w każdych okolicznościach, dlatego procedura musi rozpoznawać rodzaj żądania.

Prawo do sprostowania pozwala żądać poprawienia danych nieprawidłowych i uzupełnienia danych niekompletnych z uwzględnieniem celu przetwarzania. Prawo do ograniczenia może czasowo „zamrozić” określone operacje w przypadkach przewidzianych w art. 18 RODO.

Prawo do przenoszenia danych z art. 20 ma określony zakres. Dotyczy danych dostarczonych przez osobę, gdy przetwarzanie opiera się na zgodzie lub umowie i odbywa się w sposób zautomatyzowany. Nie jest ogólnym prawem do eksportu całej dokumentacji przedsiębiorstwa.

W systemach warto przewidzieć statusy pozwalające ograniczyć przetwarzanie bez przypadkowego usunięcia danych.

Jeżeli organizacja realizuje prawa ręcznie, instrukcja powinna jasno wskazywać różnice między żądaniami.

Czy system pozwala oznaczyć dane jako ograniczone?

Czy potrafisz poprawić dane we wszystkich istotnych systemach?

Czy eksport danych ma format nadający się do odczytu maszynowego, gdy prawo do przenoszenia ma zastosowanie?

Jeżeli przetwarzanie opiera się na art. 6 ust. 1 lit. e lub f RODO, osoba może w określonych warunkach wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją. Administrator musi wtedy ocenić, czy istnieją ważne prawnie uzasadnione podstawy nadrzędne wobec interesów, praw i wolności osoby albo podstawy do ustalenia, dochodzenia lub obrony roszczeń.

W marketingu bezpośrednim reguła jest ostrzejsza. Jeżeli osoba wnieśli sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych nie wolno już przetwarzać do takich celów.

W praktyce system marketingowy powinien potrafić zapisać sprzeciw i blokować ponowne dodanie osoby do kampanii. Usunięcie rekordu bez listy blokującej może paradoksalnie doprowadzić do ponownego importu i kolejnego kontaktu.

Rozróżniaj sprzeciw, cofnięcie zgody i wypisanie z kanału.

Nie żądaj uzasadnienia sprzeciwu wobec marketingu bezpośredniego.

Jak przeprowadzić kwalifikację prawną

- Jakiego prawa dotyczy żądanie?
- Czy zachodzi wyjątek ograniczający obowiązek administratora?
- Czy odpowiedź nastąpi w terminie i zostanie udokumentowana?

13. Wyciek danych. Pierwsze 72 godziny.

Naruszenie ochrony danych osobowych jest pojęciem z art. 4 pkt 12 RODO. Obowiązek zgłoszenia organowi nadzorczemu określa art. 33, a zawiadomienia osoby art. 34. Termin 72 godzin dotyczy zgłoszenia organowi od stwierdzenia naruszenia, jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Jedno kliknięcie może stać się naruszeniem ochrony danych.

Wysłanie wiadomości lub załącznika do niewłaściwej osoby jest klasycznym przykładem naruszenia poufności. To, że odbiorca obiecuje usunąć wiadomość, może mieć znaczenie dla oceny ryzyka, ale nie powoduje automatycznie, że naruszenia nie było.

Pierwsze działania powinny ograniczać skutki: próba wycofania wiadomości, kontakt z błędnym odbiorcą, prośba o usunięcie i potwierdzenie, zabezpieczenie dowodów oraz ustalenie zakresu danych. Następnie administrator ocenia ryzyko dla osób i obowiązki z art. 33 oraz 34 RODO.

Po incydencie warto usunąć przyczynę systemową. Jeżeli błąd wynikał z autouzupełniania adresów, podobnych nazw plików lub masowej wysyłki przez DW, samo pouczenie pracownika nie rozwiązuje problemu.

Wprowadź działanie zapobiegające powtórzeniu.

Nie każde naruszenie wymaga zgłoszenia, ale każde wymaga świadomej oceny.

Zgodnie z art. 33 ust. 1 RODO administrator zgłasza naruszenie organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie

później niż 72 godziny po jego stwierdzeniu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Jeżeli zgłoszenie następuje po 72 godzinach, trzeba wyjaśnić przyczyny opóźnienia. UODO w 2026 r. nadal egzekwuje ten obowiązek. W jednej ze spraw dotyczących wspólnoty mieszkaniowej nałożono karę za brak zgłoszenia bez zbędnej zwłoki po błędnym udostępnieniu danych członka wspólnoty.

Organizacja powinna mieć procedurę, która pozwala pracownikowi natychmiast zgłosić zdarzenie wewnętrznie. Największym wrogiem terminu 72 godzin jest sytuacja, w której informacja krąży między działami bez osoby odpowiedzialnej za decyzję.

Zgłoszenie do UODO i zawiadomienie osoby to dwa odrębne obowiązki.

Art. 34 RODO przewiduje zawiadomienie osoby bez zbędnej zwłoki, gdy naruszenie może powodować wysokie ryzyko naruszenia jej praw lub wolności. Komunikat powinien być napisany jasnym i prostym językiem oraz opisywać charakter naruszenia, kontakt do właściwego punktu, możliwe konsekwencje i zastosowane lub proponowane środki zaradcze.

Zawiadomienie ma pozwolić osobie się chronić. Dlatego zamiast ogólnego „doszło do incydentu” warto podać konkretne działania adekwatne do ryzyka, na przykład zmianę hasła, wzmożoną ostrożność wobec phishingu czy inne środki właściwe dla ujawnionych danych.

RODO przewiduje wyjątki od obowiązku indywidualnego zawiadomienia w określonych sytuacjach, między innymi gdy zastosowano skuteczne środki uniemożliwiające odczyt danych

osobom nieuprawnionym albo późniejsze działania wyeliminowały wysokie ryzyko.

Przygotuj prosty wzór komunikatu kryzysowego.

Nie ukrywaj praktycznych informacji potrzebnych do ograniczenia szkody.

Brak zgłoszenia do UODO nie oznacza braku dokumentacji zdarzenia.

Art. 33 ust. 5 RODO nakłada obowiązek dokumentowania naruszeń ochrony danych, obejmującego okoliczności naruszenia, jego skutki i podjęte działania zaradcze. Dokumentacja ma umożliwić organowi nadzorczemu weryfikację przestrzegania przepisu.

Rejestr naruszeń powinien zawierać co najmniej daty, opis zdarzenia, kategorie i zakres danych, liczbę osób w miarę możliwości, ocenę ryzyka, decyzję o zgłoszeniu lub braku zgłoszenia, informację o zawiadomieniu osób i działania naprawcze.

Dobrze prowadzony rejestr pokazuje też powtarzające się źródła błędów. Jeżeli co miesiąc występują pomyłki przy wysyłce, problem nie jest jednostkowy. To sygnał do zmiany procesu, narzędzia albo szkolenia.

Co kwartał analizuj powtarzające się przyczyny.

Pierwsza godzina ma służyć ustaleniu faktów i ograniczeniu szkody.

Po otrzymaniu zgłoszenia zapisz czas, osobę zgłaszającą i źródło informacji. Zabezpiecz logi i dowody. Ogranicz dalszy dostęp lub ujawnienie, ale nie niszczyć materiału potrzebnego do analizy. Ustal jakie dane, ilu osób i komu zostały ujawnione lub utracone.

Następnie oceń możliwe skutki dla osób. Weź pod uwagę charakter danych, możliwość identyfikacji, liczbę osób, szczególne okoliczności

i środki ograniczające skutki. Zapisz decyzję dotyczącą zgłoszenia do UODO oraz zawiadomienia osób. Jeśli informacje nie są jeszcze kompletne, pamiętaj, że RODO pozwala w określonych warunkach przekazywać informacje etapami bez dalszej zbędnej zwłoki.

Po opanowaniu incydentu wykonaj analizę przyczyny źródłowej i przypisz działania naprawcze. Zamknięcie zgłoszenia bez usunięcia przyczyny prowadzi do powtarzalnych naruszeń.

Jak przeprowadzić kwalifikację prawną

- Czy doszło do naruszenia poufności, integralności lub dostępności?
- Jakie jest ryzyko dla praw i wolności osób?
- Czy spełnione są progi z art. 33 i 34 RODO?

14. Bezpieczeństwo danych bez budowania bunkra.

Art. 32 RODO nie tworzy zamkniętego katalogu zabezpieczeń. Nakazuje dobrać środki techniczne i organizacyjne odpowiednie do ryzyka, uwzględniając między innymi stan wiedzy technicznej, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania. Z perspektywy prawnej kluczowe jest wykazanie procesu oceny ryzyka i adekwatności przyjętych środków.

Środki mają odpowiadać ryzyku, a nie modzie technologicznej.

Art. 32 RODO wymaga uwzględnienia stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka dla praw i wolności osób. Oznacza to podejście oparte na ryzyku, a nie uniwersalną checklistę identyczną dla każdej organizacji.

W zależności od sytuacji odpowiednie mogą być między innymi szyfrowanie, pseudonimizacja, odporność systemów, kopie zapasowe, testowanie zabezpieczeń, MFA, kontrola uprawnień, aktualizacje, logowanie zdarzeń i procedury reagowania. Równie ważne są działania organizacyjne: szkolenia, zasady pracy z dokumentami, weryfikacja odbiorców i zarządzanie dostawcami.

Analiza ryzyka powinna uwzględniać skutki dla osób, a nie tylko dla firmy. Utrata reputacji przedsiębiorstwa jest ważna biznesowo, ale w RODO centralne jest ryzyko dla praw i wolności osób fizycznych.

Dokumentacja papierowa zawierająca dane osobowe także może podlegać RODO, jeżeli tworzy uporządkowany zbiór lub jest częścią systemu przetwarzania. Ryzyka są prozaiczne: dokument zostawiony

na recepcji, otwarta szafa, wydruk w drukarce, przesyłka do złego adresata.

Zasady czystego biurka, zamykane szafy, kontrola kluczy, bezpieczne niszczenie i prawidłowe adresowanie przesyłek są równie ważne jak zabezpieczenia cyfrowe. Retencja papieru powinna być spójna z retencją elektroniczną.

Przy digitalizacji ustal, czy papierowy oryginał musi być nadal przechowywany na podstawie przepisów sektorowych. Nie niszczy dokumentu tylko dlatego, że został zeskanowany, jeżeli prawo wymaga oryginału.

Nie zostawiaj wydruków w urządzeniach wspólnych.

Jak przeprowadzić kwalifikację prawną

- Jakie ryzyko ma ograniczać dany środek?
- Czy administrator może wykazać adekwatność zabezpieczeń?
- Czy środki są okresowo testowane i oceniane?

15. AI w firmie a dane osobowe.

Wykorzystanie systemu AI nie wyłącza stosowania RODO. Jeżeli w procesie występują dane osobowe, należy ustalić role stron, cele, podstawy prawne, zakres danych, obowiązki informacyjne, retencję, transfery oraz ryzyko. Szczególnego znaczenia nabierają art. 22 i 35 RODO. W sierpniu 2026 r. UODO opublikował pytania inicjalne dotyczące oceny zgodności systemów AI z zasadami RODO, zastrzegając, że nie zastępują one analizy ryzyka ani DPIA.

Wklejenie danych klienta do modelu AI jest operacją przetwarzania, jeśli treść zawiera dane osobowe.

Przed wdrożeniem narzędzia AI ustal do czego ma służyć, jakie dane będą do niego trafiać, czy dostawca działa jako procesor czy w innej roli, czy dane są wykorzystywane do trenowania lub ulepszania usługi, gdzie są przetwarzane i kto jest podprocesorem. Dopiero wtedy można ocenić podstawę prawną, obowiązek informacyjny, transfery i bezpieczeństwo.

UODO w sierpniu 2026 r. opublikował pytania inicjalne dla organizacji wdrażających AI i podkreślił, że nie zastępują one analizy ryzyka, DPIA ani oceny wpływu na prawa podstawowe. To dobry sygnał praktyczny: zgodność trzeba badać przed wdrożeniem, a nie dopiero po tym, gdy pracownicy zaczną korzystać z narzędzia.

Najprostsza zasada dla zespołu brzmi: nie wklejaj danych osobowych, tajemnic i dokumentów klienta do niezatwierdzonego narzędzia. Organizacja powinna prowadzić listę zatwierdzonych zastosowań i dostawców.

Sprawdź warunki wykorzystania danych przez dostawcę AI.

Ustal dozwolone i zabronione kategorie danych wejściowych.

Oceń transfery, retencję i możliwość usunięcia danych.

Automatyzacja nie obniża standardu ochrony danych zdrowotnych ani innych danych z art. 9 RODO.

Jeżeli narzędzie AI ma analizować dokumentację medyczną, nagrania pacjentów, zdjęcia zmian skórnych, informacje o niepełnosprawności lub inne dane szczególnych kategorii, trzeba ocenić zarówno przesłanki z art. 9, jak i zwiększone ryzyko wynikające z charakteru danych.

W praktyce szczególnie ważne są minimalizacja, pseudonimizacja, kontrola dostępu, umowa z dostawcą, transfery, retencja promptów i odpowiedzi oraz możliwość wykorzystywania danych do dalszego trenowania. Należy też ustalić, czy wynik narzędzia staje się elementem decyzji dotyczącej osoby i jaki jest udział człowieka.

Nie zakładaj, że usunięcie imienia i nazwiska zawsze anonimizuje treść. Szczegółowy opis zdarzenia medycznego, data, placówka i inne cechy mogą nadal pozwolić zidentyfikować osobę.

Rozważ pseudonimizację przed wysłaniem danych do dostawcy.

Nie każde użycie algorytmu jest decyzją z art. 22 RODO, ale nie wolno pomijać tego pytania.

Art. 22 RODO dotyczy prawa osoby, aby nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, która wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa, z zastrzeżeniem wyjątków przewidzianych w przepisie.

Analizując system scoringowy, rekrutacyjny, antyfraudowy czy personalizujący ofertę, ustal, czy decyzja jest faktycznie wyłącznie automatyczna, jaki ma wpływ na osobę, jakie dane i logika są używane oraz jakie zabezpieczenia zapewniono. W określonych przypadkach znaczenie ma prawo do interwencji człowieka i zakwestionowania decyzji.

Obowiązek przejrzystości nie oznacza konieczności ujawnienia całego kodu źródłowego. Osoba powinna jednak otrzymać wymagane prawem informacje o zautomatyzowanym podejmowaniu decyzji, w tym istotne informacje o zasadach i znaczeniu oraz przewidywanych konsekwencjach, gdy przepisy tego wymagają.

Zidentyfikuj decyzje podejmowane bez realnego udziału człowieka.

Zapewnij procedurę interwencji człowieka, gdy jest wymagana.

Jak przeprowadzić kwalifikację prawną

- Czy system AI przetwarza dane osobowe i w jakich celach?
- Czy dochodzi do zautomatyzowanego podejmowania decyzji z art. 22?
- Czy proces może wymagać DPIA i analizy transferu?

16. Czy potrzebujesz IOD (inspektor ochrony danych osobowych) i DPIA (Data Protection Impact Assessment).

Obowiązek wyznaczenia inspektora ochrony danych wynika z art. 37 RODO. Nie każda firma musi mieć IOD. Ocena skutków dla ochrony danych z art. 35 ma natomiast charakter procesowy i jest wymagana wtedy, gdy dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Ocena skutków dla ochrony danych jest narzędziem dla procesów mogących powodować wysokie ryzyko.

Art. 35 RODO wymaga przeprowadzenia oceny skutków dla ochrony danych, gdy dany rodzaj przetwarzania, zwłaszcza z użyciem nowych technologii i z uwzględnieniem charakteru, zakresu, kontekstu i celów, może powodować wysokie ryzyko naruszenia praw lub wolności osób.

RODO wskazuje przykłady, w tym systematyczną i kompleksową ocenę czynników osobowych opartą na zautomatyzowanym przetwarzaniu, przetwarzanie na dużą skalę szczególnych kategorii danych oraz systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie. Znaczenie mają też wykazy organu nadzorczego.

DPIA nie jest formularzem do podpisu po zakupie systemu. Powinna poprzedzać wdrożenie i wpływać na projekt. Opisuje proces, potrzebę i proporcjonalność, ryzyka dla osób oraz środki ograniczające te ryzyka.

Czy nowy proces może powodować wysokie ryzyko?

Czy wykorzystuje nowe technologie lub szczególnie wrażliwe dane?

Czy ocena została wykonana przed uruchomieniem?

Nie każda organizacja musi wyznaczyć inspektora ochrony danych.

Art. 37 ust. 1 RODO wskazuje przypadki obowiązkowego wyznaczenia IOD. Dotyczy to między innymi organów i podmiotów publicznych, z określonym wyjątkiem dotyczącym sądów, a także sytuacji, gdy główna działalność polega na regularnym i systematycznym monitorowaniu osób na dużą skalę albo na przetwarzaniu na dużą skalę szczególnych kategorii danych lub danych z art. 10.

Mała firma może więc nie mieć obowiązku wyznaczenia IOD. Może jednak zrobić to dobrowolnie. Jeśli formalnie wyznacza IOD, trzeba respektować wymagania RODO dotyczące jego statusu, zadań, niezależności i konfliktu interesów.

Nie nazywaj każdej osoby zajmującej się RODO „IOD”, jeśli organizacja nie chce formalnie ustanawiać tej funkcji. Można powierzyć pracownikowi koordynację ochrony danych bez nadawania mu ustawowego statusu inspektora.

Jeżeli wyznaczasz IOD, zapewnij brak konfliktu interesów.

Zadbaj o wymagane zawiadomienia i publikację danych kontaktowych.

Jak przeprowadzić kwalifikację prawną

- Czy zachodzi jedna z przesłanek obowiązkowego IOD z art. 37?
- Czy planowane przetwarzanie może powodować wysokie ryzyko?
- Czy DPIA wykonano przed rozpoczęciem procesu?

17. Kontrola UODO i odpowiedzialność.

Uprawnienia organu nadzorczego określa art. 58 RODO, a administracyjne kary pieniężne art. 83. Odpowiedzialność nie ogranicza się do kary administracyjnej. Art. 82 przewiduje prawo do odszkodowania za szkodę majątkową lub niemajątkową na warunkach wynikających z prawa unijnego. Polska ustawa o ochronie danych osobowych uzupełnia ramy proceduralne i przewiduje również przepisy karne.

Najlepsze przygotowanie do kontroli to proces, który działa przed kontrolą.

Administrator powinien być w stanie wykazać zgodność. W praktyce oznacza to spójny zestaw dowodów: mapę procesów, rejestry, klauzule, podstawy prawne, testy równowagi, umowy z procesorami, analizy ryzyka, DPIA, gdy wymagane, procedury praw osób, rejestr naruszeń, dokumentację szkoleń i dowody przeglądów uprawnień.

Nie chodzi o liczbę dokumentów. Organ może pytać o to, jak procedura działa w praktyce. Jeżeli polityka przewiduje kwartalny przegląd uprawnień, a firma nigdy go nie wykonała, dokument może wręcz ujawnić rozbieżność.

Ważna jest też współpraca z organem. Art. 31 RODO nakłada obowiązek współpracy na administratora i procesora. Odpowiedzi powinny być kompletne, terminowe i oparte na faktach.

Nie twórz dokumentów, których firma nie zamierza stosować.

Wyznacz osobę koordynującą kontakt z organem.

RODO chroni ludzi, a odpowiedzialność organizacji nie kończy się na administracyjnej karze pieniężnej.

Art. 83 RODO reguluje administracyjne kary pieniężne, ale skutki naruszenia mogą obejmować także nakazy organu, konieczność zmiany procesu, koszty obsługi incydentu, zawiadomienia osób, audytu, wsparcia prawnego i technicznego oraz utratę zaufania.

Art. 82 RODO przewiduje prawo do odszkodowania za szkodę majątkową lub niemajątkową poniesioną wskutek naruszenia rozporządzenia, przy spełnieniu przesłanek odpowiedzialności. Nie należy więc oceniać ryzyka wyłącznie przez pryzmat maksymalnej wysokości kary administracyjnej.

Dojrzała organizacja pyta nie „ile wynosi kara za brak checkboxa”, lecz „jakie prawa osoby mogą zostać naruszone i jak temu zapobiec”. Takie podejście zwykle prowadzi też do lepszych decyzji biznesowych.

Uwzględniaj koszty incydentu w analizie ryzyka.

Nie oceniaj zgodności wyłącznie przez wysokość potencjalnej kary.

Priorytetyzuj procesy o największym wpływie na ludzi.

Jak przeprowadzić kwalifikację prawną

- Czy organizacja potrafi wykazać zgodność, a nie tylko przedstawić dokumenty?
- Jakie uprawnienia naprawcze może zastosować organ?
- Czy ryzyko obejmuje również roszczenia osób z art. 82 RODO?

18. Audyt RODO własnej firmy w jeden dzień.

Audyt prawny RODO powinien badać zgodność stanu faktycznego z normami, a nie tylko obecność dokumentów. Punktem odniesienia są przede wszystkim art. 5, 6, 9, 12–22, 24–25, 28, 30, 32–35 i 44–49 RODO. Wynikiem audytu powinna być lista niezgodności, ocena ich ryzyka i plan naprawczy.

Zacznij od rzeczywistości, nie od segregatora.

Pierwsze 30 minut poświęć na kanały wejścia danych. Otwórz stronę, formularze, system rezerwacji, sklep, skrzynkę kontaktową, CRM, platformę płatniczą i narzędzia reklamowe. Zapisz jakie dane wpływają i dokąd trafiają.

Kolejne 30 minut przeznacz na dostawców i dostęp. Sprawdź kto hostuje dane, kto obsługuje księgowość, mailing, płatności, chmurę i AI. Zapisz role stron, podprocesorów i lokalizacje. Następnie przejrzyj konta użytkowników i sprawdź, czy były pracownik nadal ma dostęp.

Ostatnie 30 minut wykorzystaj na retencję i incydenty. Wybierz pięć najważniejszych kategorii danych i zapytaj, kiedy są usuwane. Otwórz rejestr naruszeń. Jeśli nie istnieje, sprawdź czy w ostatnim roku były błędne wysyłki, utracone urządzenia, phishing lub przypadkowe publikacje.

Teraz porównaj to, co odkryłeś, z dokumentacją.

Weź politykę prywatności i zaznacz wszystkie cele, podstawy, odbiorców, transfery i okresy retencji. Porównaj je z mapą |z poprzedniego etapu. Każda rozbieżność trafia na listę działań.

Następnie sprawdź rejestr czynności przetwarzania i umowy powierzenia. Czy nowy dostawca newslettera jest ujęty? Czy system AI pojawił się w analizie? Czy lista podprocesorów odpowiada temu, co wynika z dokumentacji dostawcy? Czy klauzula dla kandydatów odpowiada obecnemu formularzowi rekrutacyjnemu?

Na końcu wybierz trzy procedury i poproś pracownika, aby opisał co zrobiłby w praktyce. Dobrym testem jest naruszenie, żądanie usunięcia danych i odejście pracownika. Jeśli odpowiedź różni się od dokumentu, popraw proces albo dokument.

Nadaj każdej rozbieżności właściciela i termin.

Najpierw napraw ryzyka wysokie, potem kosmetykę dokumentów.

Poniższa lista nie zastępuje analizy prawnej, ale pozwala szybko wykryć podstawowe luki.

Organizacja powinna mieć aktualną mapę procesów i systemów, przypisane cele i podstawy prawne, przejrzyste klauzule informacyjne, reguły retencji, rejestr czynności tam, gdzie jest wymagany, kontrolę procesorów i podprocesorów, procedurę praw osób, procedurę naruszeń, adekwatne zabezpieczenia oraz sposób zatwierdzania nowych narzędzi.

W obszarze marketingu trzeba rozdzielić RODO od wymagań Prawa komunikacji elektronicznej. W obszarze danych szczególnych kategorii trzeba dodatkowo wskazać przesłankę z art. 9 RODO. W obszarze AI należy ocenić dostawcę, dane wejściowe, cele, transfery, retencję i ryzyko.

Checklista powinna być przeglądana okresowo oraz przy istotnych zmianach. Nowy system, nowa kampania, wejście na nowy rynek,

zmiana dostawcy lub rozpoczęcie przetwarzania danych zdrowotnych mogą wymagać ponownej analizy.

Jak przeprowadzić kwalifikację prawną

- Czy audyt obejmuje stan faktyczny?
- Czy każda niezgodność ma wskazaną normę prawną?
- Czy plan naprawczy ma priorytety i odpowiedzialne osoby?

19. 25 błędów RODO, które możesz znaleźć we własnej firmie.

Najczęstsze błędy nie wynikają z braku jednego dokumentu, lecz z niewłaściwej kwalifikacji prawnej procesu. Do typowych należą: zbieranie zgód „na wszelki wypadek”, brak odrębnej przesłanki z art. 9, nadmierna retencja, utożsamianie każdego dostawcy z procesorem, brak analizy transferu, niewłaściwe rozpoznawanie żądań osób oraz automatyczne zgłaszanie albo niezgłaszanie każdego incydentu.

Niektóre zdania w firmie powinny natychmiast uruchamiać dodatkowe pytania.

„Mamy zgodę, więc możemy”. „Każdy ma dostęp, bo jesteśmy małym zespołem”. „Nie usuwamy, bo dysk jest duży”. „Dostawca jest znany, więc na pewno jest zgodny”. „RODO nie dotyczy danych firmowych”. „To tylko adres IP”. „Wklejam do AI, ale bez nazwiska”. „Nie zgłaszamy, bo klient jeszcze się nie skarżył”. „Politykę mamy z generatora”. „Nie mamy IOD, więc nikt nie odpowiada za RODO”.

Każde z tych zdań upraszcza problem. RODO wymaga kontekstu, celu, podstawy, proporcjonalności, bezpieczeństwa i rozliczalności. Firma nie musi tworzyć biurokracji dla samej biurokracji, ale musi umieć wyjaśnić swoje decyzje.

Najlepszym narzędziem jest kultura pytań. Zanim zespół zbierze nowe dane lub wdroży usługę, powinien zapytać: po co, jakie dane, jaka podstawa, kto ma dostęp, jak długo, jaki dostawca, jaki transfer, jakie ryzyko i jak osoba zostanie poinformowana.

Czy w firmie istnieje kanał konsultacji nowych procesów?

Czy pracownicy wiedzą, gdzie zgłaszać wątpliwości?

Czy decyzje o danych zapadają przed wdrożeniem?

Jak przeprowadzić kwalifikację prawną

- Czy problem jest błędem dokumentacyjnym czy błędą kwalifikacją procesu?
- Jaki przepis został naruszony lub może zostać naruszony?
- Jak zmienić proces, a nie tylko treść dokumentu?

20. RODO w praktyce. Plan naprawczy.

Zgodność z RODO jest procesem ciągłym. Art. 24 RODO wymaga wdrożenia odpowiednich środków oraz ich przeglądu i uaktualniania, gdy jest to potrzebne. Plan naprawczy powinien zatem łączyć korektę dokumentacji z korektą faktycznych praktyk organizacji.

RODO da się uporządkować etapami, jeśli priorytety wynikają z ryzyka.

Tydzień pierwszy: mapa danych, dostawców i dostępów. Usunąć oczywiste nadmiary, nieaktywne konta i niezatwierdzone kanały. Tydzień drugi: podstawy prawne, klauzule, marketing i umowy z kluczowymi procesorami. Tydzień trzeci: retencja, prawa osób, incydenty i rejestry. Tydzień czwarty: bezpieczeństwo, szkolenie, test procedury naruszenia i przegląd nowych technologii.

Nie próbuj jednocześnie przepisać wszystkich dokumentów. Najpierw zatrzymaj procesy, które generują największe ryzyko: publiczne udostępnienia, nadmierne uprawnienia, brak MFA, dane zdrowotne w niekontrolowanych narzędziach, marketing bez właściwej podstawy lub brak procedury incydentowej.

Każde zadanie powinno mieć właściciela, termin i dowód wykonania. „Poprawić RODO” nie jest zadaniem. „Do 15 października włączyć MFA dla administratorów CRM i zapisać potwierdzenie konfiguracji” jest.

Jedna strona pytań potrafi zatrzymać wiele błędów przed wdrożeniem.

Przed uruchomieniem nowego procesu wpisz jego nazwę i właściciela. Opisz cel biznesowy jednym zdaniem. Wskaż kategorie

osób i danych. Zaznacz, czy występują dane z art. 9 lub 10 RODO. Określ podstawę z art. 6 i ewentualną przesłankę z art. 9.

Następnie wypisz systemy, dostawców i role stron. Sprawdź podprocesorów, transfery poza EOG, okres retencji i sposób usuwania. Zdecyduj, jak spełnisz obowiązek informacyjny i jak zrealizujesz prawa osób. Oceń ryzyko i zabezpieczenia. Zastanów się, czy potrzebna jest DPIA.

Na końcu zatwierdź proces dopiero po zamknięciu krytycznych luk. Kartę zachowaj jako dowód procesu decyzyjnego i aktualizuj, jeśli zmieni się dostawca, cel lub zakres danych.

Celem nie jest firma bez danych. Celem jest firma, która wie, co robi z danymi i potrafi za to odpowiadać.

Najdojrzały system ochrony danych nie musi być najbardziej rozbudowany. Mała firma może mieć prostą dokumentację, jeżeli odpowiada ona rzeczywistym procesom, ryzyku i obowiązkom. Problem zaczyna się wtedy, gdy organizacja zbiera dane bez celu, używa ich do nowych celów bez analizy, nie kontroluje dostawców, nie usuwa danych i nie potrafi zareagować na incydent.

Wróć do pięciu pytań: po co mamy te dane, na jakiej podstawie, kto ma do nich dostęp, jak długo są potrzebne i co stanie się, jeśli je utracimy albo ujawnimy? Jeżeli odpowiedzi są konkretne i potwierdzone działaniem, firma jest znacznie bliżej realnej zgodności niż organizacja posiadająca dziesiątki wzorów dokumentów.

RODO nie kończy się po wdrożeniu. Procesy, dostawcy, prawo i technologia zmieniają się. Dlatego raz na określony czas oraz przy większych zmianach biznesowych trzeba wracać do mapy danych i aktualizować decyzje.

Traktuj incydenty i żądania osób jako test jakości systemu.

Jak przeprowadzić kwalifikację prawną

- Które ryzyka wymagają natychmiastowej reakcji?
- Które dokumenty należy zaktualizować po zmianie praktyki?
- Kiedy zaplanowano kolejny przegląd zgodności?

CHECKLISTY

Checklista audytu prawnego RODO

- ☐ Czy zidentyfikowano wszystkie cele przetwarzania?
- ☐ Czy dla każdego celu wskazano podstawę z art. 6 RODO?
- ☐ Czy dla danych szczególnych kategorii wskazano także przesłankę z art. 9 ust. 2?
- ☐ Czy obowiązki informacyjne odpowiadają faktycznym procesom?
- ☐ Czy okresy retencji mają uzasadnienie?
- ☐ Czy zweryfikowano role kontrahentów i umowy z art. 28?
- ☐ Czy zweryfikowano transfery poza EOG?
- ☐ Czy istnieje procedura obsługi praw osób?
- ☐ Czy istnieje procedura naruszeń?
- ☐ Czy przeanalizowano potrzebę DPIA i IOD?

Karta prawna nowego procesu

- ☐ Cel przetwarzania
- ☐ Kategorie osób i danych
- ☐ Podstawa z art. 6 RODO
- ☐ Ewentualna przesłanka z art. 9 ust. 2 RODO
- ☐ Źródło danych
- ☐ Odbiorcy i procesorzy
- ☐ Transfer poza EOG
- ☐ Okres retencji
- ☐ Obowiązek informacyjny
- ☐ Ryzyko i potrzeba DPIA
- ☐ Osoba odpowiedzialna za process

Checklista naruszenia

- ☐ Co się wydarzyło i kiedy?
- ☐ Kiedy administrator stwierdził naruszenie?
- ☐ Jakich danych i ilu osób dotyczy zdarzenie?
- ☐ Jakie mogą być konsekwencje dla osób?
- ☐ Jakie środki ograniczające skutki zastosowano?
- ☐ Czy istnieje ryzyko wymagające zgłoszenia z art. 33?
- ☐ Czy istnieje wysokie ryzyko wymagające zawiadomienia z art. 34?
- ☐ Czy decyzję i jej uzasadnienie udokumentowano?

Checklista prawna wdrożenia AI

- ☐ Cel użycia systemu AI
- ☐ Kategorie danych wejściowych i wyjściowych
- ☐ Rola dostawcy i organizacji
- ☐ Podstawa prawna przetwarzania
- ☐ Dane szczególnych kategorii
- ☐ Obowiązek informacyjny
- ☐ Zautomatyzowane decyzje i art. 22 RODO
- ☐ Umowa powierzenia
- ☐ Transfery poza EOG
- ☐ Retencja danych
- ☐ Ocena ryzyka i ewentualna DPIA

Podstawy prawne i źródła

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. (RODO).
- Ustawa z 10 maja 2018 r. o ochronie danych osobowych.
- Ustawa z 26 czerwca 1974 r. Kodeks pracy, w szczególności przepisy dotyczące danych kandydatów, pracowników i monitoringu.
- Ustawa z 12 lipca 2024 r. Prawo komunikacji elektronicznej, w szczególności art. 398 oraz przepisy dotyczące informacji przechowywanej w urządzeniach końcowych.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji, w zakresie w jakim proces wykorzystujący AI pozostaje równolegle objęty RODO.
- Wytyczne i opinie Europejskiej Rady Ochrony Danych, w zakresie odpowiadającym omawianym zagadnieniom.
- Materiały i decyzje Prezesa Urzędu Ochrony Danych Osobowych, w tym materiały z 2026 r. dotyczące ochrony danych w kontekście systemów sztucznej inteligencji.

Źródła urzędowe: EUR-Lex, EROD/EDPB, Urząd Ochrony Danych Osobowych oraz Internetowy System Aktów Prawnych / ELI.

Stan prawny opracowania: 7 października 2026 r.

Autor: mgr. naprawa Karolina Zuzanna Zdrojek

