

Firmowy audyt RODO 2026

Lista kontrolna zgodności i ścieżka najważniejszych zasad dla przedsiębiorcy

Lista kontrolna: zgodność z RODO

- ☐ Każde przetwarzanie ma przypisaną podstawę prawną (art. 6)
- ☐ Aktualne klauzule informacyjne w punktach zbierania danych
- ☐ Prowadzony rejestr czynności przetwarzania (RCPD)
- ☐ Umowy powierzenia z biurem rachunkowym, IT i hostingiem
- ☐ Zasada minimalizacji - zbierasz tylko potrzebne dane
- ☐ Procedura reakcji na naruszenie (72 godziny) i ewidencja naruszeń
- ☐ Procedura realizacji praw osób (dostęp, sprostowanie, usunięcie)
- ☐ Zabezpieczenia danych (dostęp, hasła, kopie zapasowe, szyfrowanie)
- ☐ Zgody na cookies i marketing - bez manipulacyjnych wzorców
- ☐ Zasady korzystania z narzędzi AI i monitoringu pracowników
- ☐ Przeszkolony zespół i wyznaczona osoba odpowiedzialna za dane

Ściąga: podstawy, prawa i terminy

Najważniejsze zasady RODO w pigułce - stan na 2026 rok.

Sześć podstaw przetwarzania (art. 6)

Podstawa	Typowy przykład w firmie
Zgoda	Newsletter, marketing, cookies inne niż niezbędne
Wykonanie umowy	Realizacja zamówienia, obsługa klienta, wysyłka
Obowiązek prawny	Faktury, dokumentacja kadrowa, rozliczenia z ZUS i US
Prawnie uzasadniony interes	Windykacja, bezpieczeństwo, marketing własny
Żywotne interesy	Ratowanie życia lub zdrowia - rzadkie w firmie
Zadanie publiczne	Zadania władzy publicznej - zwykle poza biznesem

Prawa osób, których dane dotyczą

Prawo	Na czym polega
Dostęp	Informacja, jakie dane i jak są przetwarzane
Sprostowanie	Poprawienie lub uzupełnienie danych
Usunięcie	„Bycie zapomnianym” w określonych sytuacjach
Ograniczenie	Czasowe wstrzymanie przetwarzania
Przenoszenie	Otrzymanie danych w formacie do przeniesienia
Sprzeciw	Wobec uzasadnionego interesu, w tym marketingu

Terminy i kary

Co	Wartość
Realizacja praw osób	bez zbędnej zwłoki, zwykle do 1 miesiąca
Zgłoszenie naruszenia do UODO	do 72 godzin od stwierdzenia
Maksymalna kara	20 mln euro lub 4% rocznego światowego obrotu

Materiał informacyjny, nie stanowi porady prawnej. W wątpliwej sprawie skonsultuj się z prawnikiem lub inspektorem ochrony danych.