• 20 MLN € LUB 4% OBROTU Marketing, CRM, teczki klientów, dostawcy

Ochrona danych (RODO) Przewodnik zgodności dla firm motoryzacyjnych

Zgody marketingowe, klauzule, żądania klientów, bezpieczeństwo i dostawcy: co sprawdza UODO **i dlaczego otwarta szafa z teczkami to ryzyko milionów.**





20 mln €
lub 4% obrotu – maksymalna kara RODO.

16,9 mln zł
kara UODO dla McDonald's Polska.

72 h
na zgłoszenie naruszenia do UODO.

5 standardów | 12 punktów kontroli | RODO · UODO | Dobrze / źle | Czas naprawy

2018 RODO → **2025** Rekordowa kara UODO → **Teraz** Skargi klientów → **Dane klientów to Twoja odpowiedzialność.**

PO CO TEN PRZEWODNIK

Dealer ma więcej danych niż niejeden bank.

Dowody osobiste, prawa jazdy, dane bankowe, adresy i dane z pojazdów: dealer zbiera je i przekazuje importerowi, bankom i ubezpieczycielom. RODO przewiduje kary do **20 mln euro lub 4% obrotu**.

Ten przewodnik obejmuje 5 standardów ochrony danych dla dealerów.

GDZIE POWSTAJE RYZYKO

Marketing
Zgody
DAN-01

Informacja
Klauzule
DAN-02

Prawa
Żądania klientów
DAN-03

Bezpieczeństwo
Teczki i systemy
DAN-04

Dostawcy
Umowy powierzenia
DAN-05

Retencja
Usuwanie
DAN-05

KTO EGZEKWUJE

UODO
Prezes Urzędu
Kary i nakazy

UKE / UOKiK
Marketing
Komunikacja elektroniczna

Sądy
Cywilne
Odszkodowania

Importer
Umowy
Wymogi dotyczące danych

DLA KOGO

Zarząd
Rozumie ryzyko.

Marketing i sprzedaż
Zbiera zgody prawidłowo.

IOD i audytorzy
Testują zgody i żądania.

KARA LICZONA OD ŚWIATOWEGO OBROTU

Otwarta szafa, słabe hasła. 16,9 mln zł.

UODO ukarał McDonald's Polska kwotą **16,9 mln zł** za braki w analizie ryzyka i zabezpieczeniach. Maksymalna kara to **20 mln € lub 4% obrotu**.

DRABINA KAR

POZIOM 1
Upomnienie
Pierwsza reakcja UODO.

POZIOM 2
Nakaz
Zakaz przetwarzania.

POZIOM 3
16,9 mln zł
Przykład: McDonald's Polska.

POZIOM 4
20 mln € / 4%
Maksimum.

PRAWDZIWE SPRAWY I FAKTY

KTO	WYNIK	CO SIĘ STAŁO
McDonald's Polska UODO	**16,9 mln zł**	Braki w analizie ryzyka i zabezpieczeniach.
RODO Maksimum	**4%** obrotu	Lub 20 mln €, co wyższe.
Marketing PKE	**Zgoda**	Odrębna zgoda na SMS i e-mail.

NARUSZENIE
72 h
Na zgłoszenie do UODO.

KARA
4%
Światowego obrotu.

A POTEM
Pozwy
Klienci **żądają odszkodowań**.

JAK KORZYSTAĆ Z PRZEWODNIKA

Jedna strona na standard. Zgoda to podstawa.

1. **Nagłówek**: kod, obszar, osoba odpowiedzialna, maksymalna kara
2. **Przepisy**: jaki organ i jakie przepisy
3. **Koszt**: kara, inne skutki i prawdziwa sprawa
4. **Dobrze / źle**: ilustracje i sposób audytu

STANDARDY W PRZEWODNIKU: 5

DAN-01	Zgody marketingowe	RODO art. 6–7	KRYTYCZNE	20 mln € / 4%	Natychmiast	5
DAN-02	Klauzula informacyjna	RODO art. 13	KRYTYCZNE	20 mln € / 4%	30 dni	6
DAN-03	Prawa klientów	RODO art. 15–22	KRYTYCZNE	20 mln € / 4%	7 dni	7
DAN-04	Bezpieczeństwo danych	RODO art. 32–33	KRYTYCZNE	20 mln € / 4%	24 godziny	8
DAN-05	Umowy powierzenia i retencja	RODO art. 28	KRYTYCZNE	20 mln € / 4%	30 dni	9

IDEALNY CZAS NAPRAWY · LICZONY OD PRZESŁANIA AUDYTU

Natychmiast	Zatrzymaj od razu · poważne ryzyko lub oczywiste naruszenie	1 std.
24 godziny	Napraw w ciągu 1 dnia roboczego	1 std.
7 dni	Napraw w ciągu tygodnia · dokumenty, szkolenia	1 std.
30 dni	Zaplanuj i zamknij w miesiąc · procedury i systemy	2 std.

OCENA PUNKTÓW KONTROLI

ZGODNE

Wszystkie kryteria spełnione w chwili audytu, z zebranymi dowodami.

NIEZGODNE

Któreś kryterium niespełnione w chwili audytu. Zapisz, co widziałeś i kto odpowiada za naprawę.

N/D

Tylko gdy wyklucza to pole „Kiedy dotyczy". Zapisz powód.

Uwaga. Dane przekazywane importerowi wymagają podstawy prawnej i muszą być opisane w klauzuli.

DAN-01 DANE OSOBOWE · UODO · STANDARD 01 Z 05

Zgody marketingowe

Obszar **Marketing · CRM** | Odpowiada **Kierownik marketingu · IOD** | Organ **UODO**

MAKSYMALNA KARA

20 mln €

lub 4% światowego obrotu

Co wyższe · plus **odszkodowania** dla klientów

• KRYTYCZNE

PRZEPISY

RODO

RODO (rozporządzenie UE 2016/679) · **Ustawa o ochronie danych osobowych** z 2018 r. · **RODO art. 6–7** · **Prawo komunikacji elektronicznej** – zgoda na marketing

CO SPRAWDZAMY

SMS-y i e-maile marketingowe trafiają tylko do klientów, którzy wyrazili odrębną, niezaznaczoną domyślnie zgodę, a rezygnacja jest prosta.

PUNKTY KONTROLI W AUDYCIE

- P1 Czy zgoda marketingowa jest odrębna i niezaznaczona domyślnie?
- P2 Czy każda wiadomość ma prosty sposób rezygnacji?
- P3 Czy rezygnacje trafiają do wszystkich systemów?

ILE KOSZTUJE NIEZGODNOŚĆ

KARA

Kary RODO sięgają **20 mln euro lub 4% światowego obrotu**, zależnie od tego, która kwota jest wyższa.

POZA KARĄ

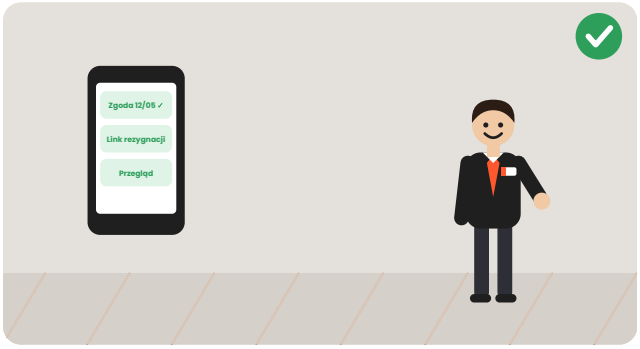
Prezes UODO może też **zakazać przetwarzania** danych. Klienci mogą dochodzić odszkodowania.

EGZEKWOWANIE W PRAKTYCE

Zgoda

Marketing SMS i e-mail wymaga **odrębnej zgody** (Prawo komunikacji elektronicznej).

✔ DOBRZE



Odrębna zgoda i rezygnacja.

✖ ŹLE

20 MLN € / 4%



Zgoda ukryta w regulaminie.

CEL

Marketing bez zgody to najczęstsza skarga na dealerów.

NAPRAW W CIĄGU

◷ Natychmiast

KRYTERIA AUDYTU · ZGODNE, GDY

- Odrębna zgoda
- Rezygnacja
- Synchronizacja systemów

JAK NAJLEPIEJ AUDYTOWAĆ

1. Sprawdź formularze
2. Przetestuj rezygnację

Dowody: Formularze + test.

NAJGORSZY SCENARIUSZ Kara do **20 mln €** lub 4% obrotu.

DAN-02 DANE OSOBOWE · UODO · STANDARD 02 Z 05

Klauzula informacyjna

Obszar **Sprzedaż · Serwis** | Odpowiada **IOD** | Organ **UODO**

MAKSYMALNA KARA

20 mln €

lub 4% światowego obrotu

Co wyższe · plus **odszkodowania** dla klientów

• KRYTYCZNE

PRZEPISY

RODO

RODO (rozporządzenie UE 2016/679) · **Ustawa o ochronie danych osobowych** z 2018 r. · **RODO art. 13–14** – obowiązek informacyjny

CO SPRAWDZAMY

Klient wie, jakie dane zbieramy, po co, komu je przekazujemy (importer, banki, ubezpieczyciele) i jak długo je przechowujemy.

PUNKTY KONTROLI W AUDYCIE

- P1 Czy klauzula jest przekazywana przy każdym zbieraniu danych?
- P2 Czy wymienia importera, banki i ubezpieczycieli?

ILE KOSZTUJE NIEZGODNOŚĆ

KARA

Kary RODO sięgają **20 mln euro lub 4% światowego obrotu**, zależnie od tego, która kwota jest wyższa.

POZA KARĄ

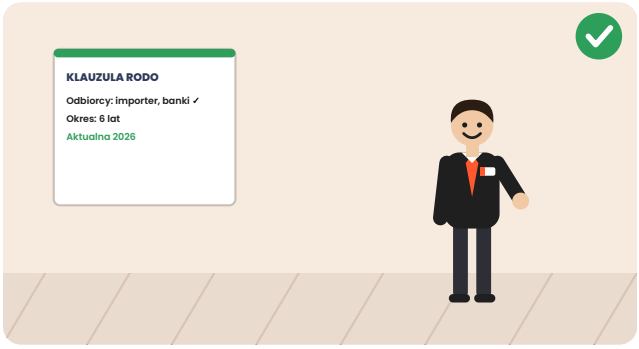
Prezes UODO może też **zakazać przetwarzania** danych. Klienci mogą dochodzić odszkodowania.

EGZEKWOWANIE W PRAKTYCE

4%

światowego obrotu – maksymalna kara RODO, wyższa z dwóch wartości.

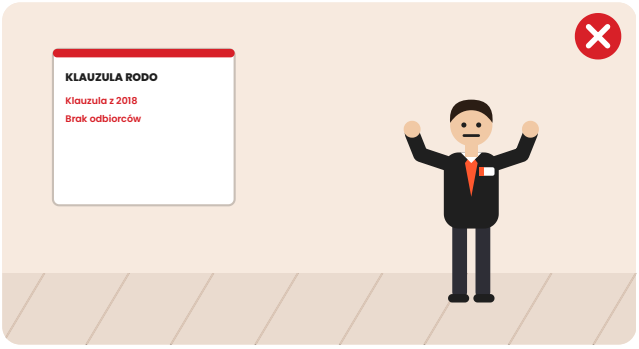
✔ DOBRZE



Aktualna klauzula z odbiorcami.

✖ ŹLE

20 MLN € / 4%



Klauzula z 2018 bez odbiorców.

CEL

Dealer przekazuje dane wielu podmiotom – klient musi o tym wiedzieć.

NAPRAW W CIĄGU

◷ 30 dni

KRYTERIA AUDYTU · ZGODNE, GDY

- Klauzula wszędzie
- Wszyscy odbiorcy
- Aktualna

JAK NAJLEPIEJ AUDYTOWAĆ

1. Zbierz klauzule z kanałów

Dowody: Klauzule.

NAJGORSZY SCENARIUSZ Kara do **20 mln €** lub 4%.

DAN-03 DANE OSOBOWE · UODO · STANDARD 03 Z 05

Prawa klientów

Obszar **Obsługa klienta** | Odpowiada **IOD** | Organ **UODO**

MAKSYMALNA KARA

20 mln €

lub 4% światowego obrotu

Co wyższe · plus **odszkodowania** dla klientów

• KRYTYCZNE

PRZEPISY

RODO

RODO (rozporządzenie UE 2016/679) · **Ustawa o ochronie danych osobowych** z 2018 r. · **RODO art. 12, 15–22** – żądania osób, których dane dotyczą

CO SPRAWDZAMY

Żądania dostępu, sprostowania, usunięcia i sprzeciwu są rejestrowane i realizowane w ciągu miesiąca.

PUNKTY KONTROLI W AUDYCIE

P1 Czy żądania są rejestrowane?

P2 Czy odpowiedź trafia w ciągu miesiąca?

ILE KOSZTUJE NIEZGODNOŚĆ

KARA

Kary RODO sięgają **20 mln euro lub 4% światowego obrotu**, zależnie od tego, która kwota jest wyższa.

POZA KARĄ

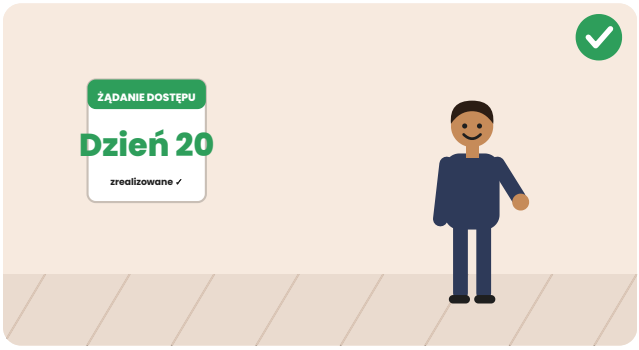
Prezes UODO może też **zakazać przetwarzania** danych. Klienci mogą dochodzić odszkodowania.

EGZEKWOWANIE W PRAKTYCE

4%

światowego obrotu – maksymalna kara RODO, wyższa z dwóch wartości.

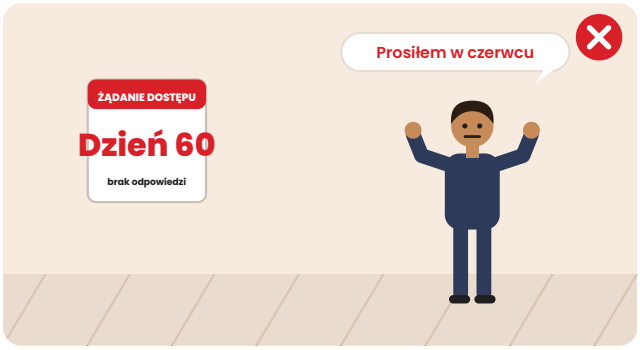
✔ DOBRZE



Odpowiedź w 20 dni.

✖ ŹLE

20 MLN € / 4%



Brak odpowiedzi po 60 dniach.

CEL

Skargi do UODO zaczynają się od nieodpowiedzianych żądań.

NAPRAW W CIĄGU

◷ 7 dni

KRYTERIA AUDYTU · ZGODNE, GDY

- Rejestr żądań
- Miesiąc na odpowiedź

JAK NAJLEPIEJ AUDYTOWAĆ

1 Sprawdź rejestr

Dowody: Rejestr żądań.

NAJGORSZY SCENARIUSZ Skarga do UODO i kara **do 20 mln €**.

DAN-04 DANE OSOBOWE · UODO · STANDARD 04 Z 05

Bezpieczeństwo danych

Obszar **Salon · IT** | Odpowiada **Kierownik IT** | Organ **UODO**

MAKSYMALNA KARA

20 mln €

lub 4% światowego obrotu

Co wyższe · plus **odszkodowania** dla klientów

• KRYTYCZNE

PRZEPISY

RODO

RODO (rozporządzenie UE 2016/679) · **Ustawa o ochronie danych osobowych** z 2018 r. · **RODO art. 32–34** – bezpieczeństwo i zgłaszanie naruszeń w 72 godziny

CO SPRAWDZAMY

Dokumenty klientów (dowody osobiste, prawa jazdy, dane bankowe) są zabezpieczone, systemy mają MFA, a naruszenia są zgłaszane do UODO w 72 godziny.

PUNKTY KONTROLI W AUDYCIE

- P1 Czy teczki klientów są zamykane na klucz?
- P2 Czy DMS i CRM mają uwierzytelnianie dwuskładnikowe?
- P3 Czy jest procedura zgłaszania naruszeń w 72 h?

ILE KOSZTUJE NIEZGODNOŚĆ

KARA

Kary RODO sięgają **20 mln euro lub 4% światowego obrotu**, zależnie od tego, która kwota jest wyższa.

POZA KARĄ

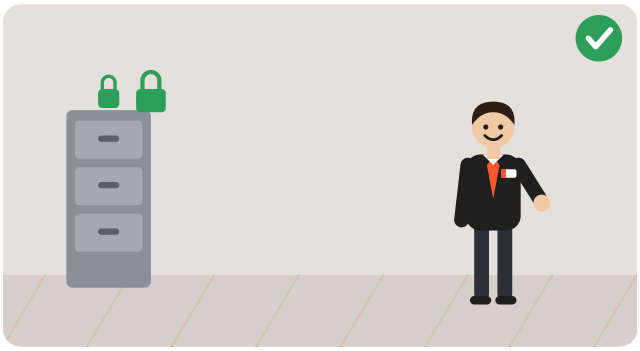
Prezes UODO może też **zakazać przetwarzania** danych. Klienci mogą dochodzić odszkodowania.

EGZEKWOWANIE W PRAKTYCE

16,9 mln zł

kara UODO dla **McDonald's Polska** za braki w analizie ryzyka i zabezpieczeniach danych.

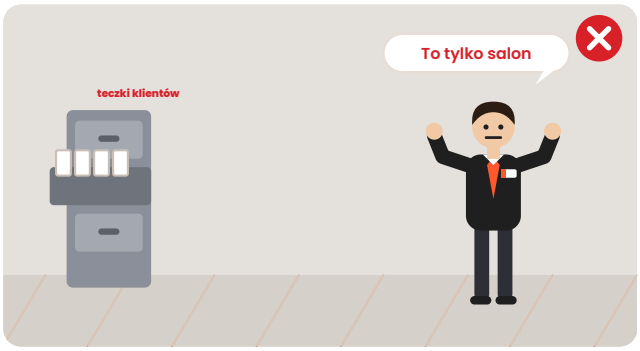
✔ DOBRZE



Szafa zamknięta, MFA.

✖ ŹLE

20 MLN € / 4%



Otwarta szafa z teczkami.

CEL

Kara dla McDonald's dotyczyła właśnie zabezpieczeń.

NAPRAW W CIĄGU

24 godziny

KRYTERIA AUDYTU · ZGODNE, GDY

- Zamknięte teczki
- MFA
- Procedura 72 h

JAK NAJLEPIEJ AUDYTOWAĆ

1. Obejdź salon
2. Sprawdź MFA

Dowody: Zdjęcia + ustawienia.

NAJGORSZY SCENARIUSZ Kara jak dla McDonald's: **16,9 mln zł**, plus roszczenia klientów.

DAN-05 DANE OSOBOWE · UODO · STANDARD 05 Z 05

Umowy powierzenia i retencja

Obszar **Zarząd · IT** | Odpowiada **IOD** | Organ **UODO**

MAKSYMALNA KARA

20 mln €

lub 4% światowego obrotu

Co wyższe · plus **odszkodowania** dla klientów

• KRYTYCZNE

PRZEPISY

RODO

RODO (rozporządzenie UE 2016/679) · **Ustawa o ochronie danych osobowych** z 2018 r. · **RODO art. 28** umowy powierzenia · **art. 5 ust. 1 lit. e** ograniczenie przechowywania

CO SPRAWDZAMY

Dostawcy (DMS, CRM, call center) mają umowy powierzenia, a stare dane są usuwane zgodnie z harmonogramem.

PUNKTY KONTROLI W AUDYCIE

- P1 Czy każdy dostawca przetwarzający dane ma umowę powierzenia?
- P2 Czy jest harmonogram usuwania danych?

ILE KOSZTUJE NIEZGODNOŚĆ

KARA

Kary RODO sięgają **20 mln euro lub 4% światowego obrotu**, zależnie od tego, która kwota jest wyższa.

POZA KARĄ

Prezes UODO może też **zakazać przetwarzania** danych. Klienci mogą dochodzić odszkodowania.

EGZEKWOWANIE W PRAKTYCE

16,9 mln zł

kara UODO dla **McDonald's Polska** za braki w analizie ryzyka i zabezpieczeniach danych.

✔ DOBRZE



Umowy i retencja.

✖ ŹLE

20 MLN € / 4%



Brak umowy, dane od 2012.

CEL

W sprawie McDonald's ukarano też podmiot przetwarzający.

NAPRAW W CIĄGU

◷ 30 dni

KRYTERIA AUDYTU · ZGODNE, GDY

- ✓ Umowy powierzenia
- ✓ Harmonogram usuwania

JAK NAJLEPIEJ AUDYTOWAĆ

1. Sprawdź umowy
2. Sprawdź najstarsze dane

Dowody: Umowy + harmonogram.

NAJGORSZY SCENARIUSZ Kara dla administratora **i** podmiotu przetwarzającego.

POPRAW ZGODY PRZED KOLEJNĄ KAMPANIĄ

Twój 30-dniowy plan: dane.

Dziś

- [ ] **DAN-01** Zgody marketingowe
  Natychmiast
- [ ] **DAN-04** Bezpieczeństwo danych
  24 godziny

Ten tydzień

- [ ] **DAN-03** Prawa klientów
  7 dni

Ten miesiąc

- [ ] **DAN-02** Klauzula informacyjna
  30 dni
- [ ] **DAN-05** Umowy powierzenia i retencja
  30 dni

?/5 Policz zgodne punkty. Każde niezgodne może oznaczać karę **do 4% obrotu**.

ŹRÓDŁA

- EROD: kara UODO dla McDonald's Polska (4 022 773 €) · edpb.europa.eu
- RODO; Ustawa o ochronie danych osobowych (2018) · isap.sejm.gov.pl

Zastrzeżenie. Materiał pomocniczy do audytu; nie stanowi porady prawnej.

ZATWIERDZENIE AUDYTU

DEALER / LOKALIZACJA _____ AUDYTOR _____ DATA _____ WYNIK __ / 5

PODPIS DYREKTORA / WŁAŚCICIELA _____ PODPIS OSOBY ODP. ZA COMPLIANCE _____