Umowa powierzenia danych RODO

Szablon struktury umowy powierzenia przetwarzania danych osobowych według obowiązkowych klauzul z art. 28 ust. 3 RODO (podprocesorzy, środki z art. 32, audyty, retencja) w DOCX i PDF.

Stan prawny i wymagań: 2026-11-16 | Wersja pliku: 2026-11 | Licencja: CC BY 4.0 · tql.pl/pl/wzory/umowa-powierzenia-danych-rodo

1. Struktura klauzul umowy powierzenia przetwarzania danych osobowych (art. 28)

Nr	Element / Pole	Instrukcja wypełnienia	Podstawa
1	Strony umowy oraz powiązanie z umową główną świadczenia usług	Dane Administratora i Podmiotu przetwarzającego (procesora) ze wskazaniem umowy głównej (np. księgowość, SLA IT, SaaS), w ramach której dochodzi do powierzenia.	art. 28 ust. 3 zdanie pierwsze RODO
2	Przedmiot, charakter, cel oraz okres trwania przetwarzania	Opis czynności (np. hosting, serwis ERP, wsparcie kadrowo-płacowe) i wyraźne powiązanie czasu obowiązywania powierzenia z okresem trwania umowy głównej.	art. 28 ust. 3 zdanie drugie RODO
3	Rodzaj danych osobowych i kategorie osób, których dane dotyczą	Konkretny wykaz pól danych i grup osób - zaznaczyć wyraźnie, czy powierzenie obejmuje dane szczególnych kategorii z art. 9 RODO.	art. 28 ust. 3 RODO (zakres przedmiotowy)
4	Polecenia Administratora, tajemnica personelu i przekazywanie poza EOG	Zobowiązanie procesora do działania wyłącznie na udokumentowane polecenia, nadania upoważnień z klauzulą poufności oraz warunki transferu poza EOG.	art. 28 ust. 3 lit. a i b oraz art. 29 RODO
5	Załącznik środków technicznych i organizacyjnych (art. 32 RODO)	Konkretne wymogi szyfrowania w tranzycie/spoczynku, kontroli dostępu, MFA, kopii zapasowych i regularnych aktualizacji bezpieczeństwa.	art. 28 ust. 3 lit. c w zw. z art. 32 RODO
6	Zasady podpowierzenia (szczegółowa lub ogólna zgoda na podprocesorów)	Wskazanie zaakceptowanej listy podprocesorów, okna na zgłoszenie sprzeciwu przy zmianie (np. 14 dni) oraz przeniesienia tych samych obowiązków umową niższego rzędu.	art. 28 ust. 2, ust. 3 lit. d oraz ust. 4 RODO
7	Pomoc w realizacji praw osób i zgłaszaniu incydentów (okno powiadomienia)	Termin przekazania Administratorowi informacji o stwierdzonym wycieku lub	art. 28 ust. 3 lit. e i f oraz art. 33 RODO

		awarii bezpieczeństwa (zalecane <= 24h) i tryb pomocy przy wnioskach z rozdz. III.	
8	Usunięcie lub zwrot danych po zakończeniu umowy oraz prawo do audytu	Termin wydania bazy danych i protokolarnego usunięcia kopii roboczych po wygaśnięciu usług oraz zasady przeprowadzania inspekcji i audytów.	art. 28 ust. 3 lit. g i h RODO

2. Przykład wypełnienia: powierzenie danych przy obsłudze systemu CRM w chmurze

Przykład sp. z o.o. korzysta z zewnętrznej firmy wdrożeniowej utrzymującej serwer systemu relacji z klientami oraz wykonującej okresowe kopie bezpieczeństwa (uwaga: wzór ma charakter pomocniczy).

Nr	Pole	Przykładowy zapis w dokumentacji
1	Strony umowy oraz powiązanie z umową główną świadczenia usług	Administrator: Przykład sp. z o.o.; Procesor: Przykładowy Dostawca IT sp. z o.o.; podstawa: Umowa serwisowa IT nr 12/2026 z 16.11.2026 r.
2	Przedmiot, charakter, cel oraz okres trwania przetwarzania	Charakter i cel: utrzymanie serwera aplikacji CRM, wykonywanie kopii zapasowych oraz usuwanie zgłoszonych błędów oprogramowania przez okres trwania umowy głównej
3	Rodzaj danych osobowych i kategorie osób, których dane dotyczą	Kategorie osób: klienci B2B i pracownicy; dane zwykłe: imię, nazwisko, służbowy e-mail, telefon, historia zgłoszeń (bez danych art. 9 i 10 RODO)
4	Polecenia Administratora, tajemnica personelu i przekazywanie poza EOG	Procesor przetwarza dane wyłącznie w centrach danych na terenie EOG; dostęp mają tylko upoważnieni pracownicy zobowiązani pisemnie do zachowania tajemnicy bezterminowo
5	Załącznik środków technicznych i organizacyjnych (art. 32 RODO)	Połączenie szyfrowane TLS, dyski baz danych szyfrowane AES-256, obowiązkowe MFA dla kont administracyjnych i automatyczna codzienna kopia zapasowa
6	Zasady podpowierzenia (szczegółowa lub ogólna zgoda na podprocesorów)	Ogólna zgoda na podmioty z załączonego wykazu podprocesorów; zmiana podwykonawcy wymaga powiadomienia Administratora na 14 dni przed udzieleniem dostępu
7	Pomoc w realizacji praw osób i zgłaszaniu incydentów (okno powiadomienia)	Stwierdzenie naruszenia danych procesor zgłasza na adres bezpieczeństwa Administratora niezwłocznie, nie później niż w ciągu 24 godzin, wraz z wstępną oceną skutków

8	Usunięcie lub zwrot danych po zakończeniu umowy oraz prawo do audytu	W 14 dni od wygaśnięcia umowy głównej procesor eksportuje bazę dla Administratora, trwale usuwa kopie z serwerów oraz dopuszcza audyt raz w roku po uprzedzeniu na 10 dni roboczych

3. Najczęstsze błędy i sposób ich uniknięcia

Błąd	Skutek	Jak uniknąć	Podstawa
Wypełnienie zakresu danych ogólnikiem „wszelkie dane" zamiast konkretnych kategorii osób i pól	Nie można wykazać przestrzegania zasady minimalizacji danych ani prawidłowo powiązać umowy powierzenia z Rejestrem Czynności Przetwarzania.	Przenieś dokładną listę pól z modułu oprogramowania lub procesu kadrowo-księgowego prosto do załącznika nr 1 umowy.	art. 5 ust. 1 lit. c i art. 28 ust. 3 RODO
Przepisywanie w umowie identycznego terminu 72 godzin dla procesora, jaki sam Administrator ma wobec Prezesa UODO	Gdy dostawca zgłosi wyciek w 71. godzinie od stwierdzenia, Administrator zostaje zaledwie z kilkudziesięcioma minutami na analizę i zgłoszenie do UODO.	Ustal umowny termin powiadomienia dla podmiotu przetwarzającego na 12–24 godziny od wykrycia lub stwierdzenia incydentu.	art. 28 ust. 3 lit. f i art. 33 ust. 1–2 RODO
Brak jakiejkolwiek weryfikacji gwarancji technicznych dostawcy przed podpisaniem umowy (niedopełnienie art. 28 ust. 1)	Sama podpisana umowa na papierze nie chroni przed zarzutem UODO wyboru nierzetelnego procesora po włamaniu do niezabezpieczonego serwera.	Przeprowadź przed podpisaniem ankiety weryfikacyjne (lub poproś o certyfikat ISO/IEC 27001 / raport z testów kopii zapasowych) i zarchiwizuj ocenę.	art. 28 ust. 1 i art. 32 RODO
Mylenie powierzenia danych z niezależnym udostępnieniem danych (np. pomiędzy dwoma odrębnymi administratorami)	Zawieranie zbędnych umów powierzenia z podmiotami działającymi jako odrębni administratorzy (np. kurierzy pocztowi, banki, kancelarie radców prawnych co do ich zadań).	Określ rolę prawną każdej ze stron przed przygotowaniem umowy: kto ustala cele i sposoby przetwarzania, jest odrębnym administratorem, nie procesorem.	art. 4 pkt 7–8 i art. 28 RODO
Pominięcie obowiązku usunięcia albo zwrotu danych również w kopiach bezpieczeństwa po rozwiązaniu współpracy	Dane byłych pracowników i klientów krążą latami w archiwach nieużywanego już systemu dostawcy bez żadnej podstawy prawnej.	Ustal jasny termin usunięcia danych produkcyjnych oraz maksymalny cykl nadpisywania zamkniętych zaszyfrowanych kopii zapasowych po rozwiązaniu umowy.	art. 28 ust. 3 lit. g RODO

Opracował: Ireneusz Kozera, audytor wiodący ISO (TQL, www.tql.pl). Licencja CC BY 4.0: wzór ma charakter pomocniczo-informacyjny i przed wdrożeniem wymaga dopasowania do procesów i warunków konkretnej organizacji.