

Rejestr Podwykonawców

Łańcuch podwykonawców usług ICT z rangą, lokalizacjami, istotnością i przeniesieniem wymagań klienta

Rejestr ewidencjonuje podmioty, którym [NAZWA DOSTAWCY] powierza część usług świadczonych podmiotom finansowym, z rangą w łańcuchu, lokalizacjami i statusem przeniesienia wymagań. Dostarcza klientowi dane do jego rejestru informacji i jest podstawą notyfikacji zmian w łańcuchu.

WŁAŚCICIEL KOORDYNATOR BEZPIECZEŃSTWA ICT	ZATWIERDZA ZARZĄD	PRZEGLĄD CO 12 MIESIĘCY; WPIS DO 10 DNI ROBOCZYCH OD ZMIANY	CZAS CZYTANIA ≈ 12 MIN
ORGANIZACJA [NAZWA DOSTAWCY]			

1. Cel i podstawa

Umowa z klientem musi wskazywać, czy podwykonawstwo usługi wspierającej funkcję krytyczną lub istotną jest dopuszczalne i na jakich warunkach **§ DORA art. 30.2 lit. a**. Warunki te doprecyzowuje rozporządzenie delegowane (UE) 2025/532 (w mocy od 22 lipca 2025 r.): klient ocenia podwykonawstwo przed zawarciem umowy (art. 3), umowa określa warunki podwykonawstwa i przeniesienie obowiązków (art. 4), a istotne zmiany w podwykonawstwie wymagają powiadomienia klienta z wyprzedzeniem pozwalającym mu na ocenę i ewentualny sprzeciw (art. 5). Klient wpisuje łańcuch podwykonawców do swojego rejestru informacji **§ DORA art. 28.3** według wzorów z rozporządzenia wykonawczego (UE) 2024/2956, w tym rangę każdego podmiotu w łańcuchu.

ZASADA

Dostawca odpowiada wobec klienta za podwykonawców jak za własne działania. Podwykonawca, którego nie ma w rejestrze, nie dostaje dostępu do usługi, danych ani środowiska klienta.

2. Ranga w łańcuchu

Ranga opisuje odległość podmiotu od klienta. W rejestrze informacji klienta Dostawca jako bezpośredni dostawca ma rangę 1; jego bezpośredni podwykonawcy rangę 2; ich podwykonawcy rangę 3 i dalej. Dostawca ewidencjonuje rangę 2 dla wszystkich podwykonawców i rangę 3 lub dalszą tam, gdzie podmiot jest istotny dla usługi (np. centrum danych dostawcy chmury).

RANGA	KTO	PRZYKŁAD
1	[NAZWA DOSTAWCY] (strona umowy z klientem)	Software house świadczący SaaS
2	Bezpośredni podwykonawca Dostawcy	Dostawca chmury publicznej; zewnętrzny zespół programistów
3	Podwykonawca podwykonawcy	Operator centrum danych dostawcy chmury

3. Istotność podwykonawcy

Podwykonawca jest istotny, jeżeli spełnia co najmniej jedno kryterium. Podwykonawca istotny podlega pełnemu trybowi z rozdziału 4; pozostali są tylko ewidencjonowani. Przy wątpliwości traktuj podmiot jako istotny.

KRYTERIUM	PYTANIE
PW1 · Rdzeń usługi	Czy wykonuje całość lub istotną część usługi wspierającej funkcję krytyczną lub istotną klienta (np. hosting produkcji)?
PW2 · Dane klienta	Czy ma dostęp do danych klienta lub do środowiska produkcyjnego, także administracyjny lub serwisowy?
PW3 · Ciągłość i bezpieczeństwo	Czy jego awaria lub naruszenie bezpośrednio wpływa na SLA, RTO lub poufność danych klienta?
PW4 · Trudna zastępowalność	Czy zastąpienie go zajęłoby dłużej niż okres przejściowy z umowy klienta?
PW5 · Jurysdykcja lub koncentracja	Czy działa spoza EOG albo obsługuje wiele usług Dostawcy jednocześnie?

4. Zaangażowanie i zmiana podwykonawcy

1. **Ocena przed zaangażowaniem.** Koordynator Bezpieczeństwa ICT sprawdza: certyfikaty lub raporty niezależne (np. ISO 27001, SOC 2), lokalizacje, zabezpieczenia, plan ciągłości, gotowość do przyjęcia wymagań z rozdziału 5. Wynik zapisuje w rejestrze.
2. **Przeniesienie wymagań.** Umowa z podwykonawcą istotnym zawiera wymagania z rozdziału 5 (sprawdź przed podpisaniem).
3. **Notyfikacja klienta.** Zaangażowanie lub zmiana podwykonawcy istotnego dla usługi wspierającej funkcję krytyczną lub istotną: notyfikacja domyślnie 90 dni przed zmianą; pozostałe: domyślnie 30 dni, w obu przypadkach terminy domyślne i negocjowalne ([→ L3-DDS-05 · Procedura Zarządzania Zmianą](#), rozdział 5). Zmiana nie wchodzi przed upływem terminu ani wbrew sprzeciwowi.
4. **Dane osobowe.** Jeżeli podwykonawca będzie przetwarzał dane osobowe klienta, Dostawca jako podmiot przetwarzający uzyskuje uprzednią szczegółową zgodę klienta albo, przy zgodzie ogólnej, informuje klienta o zamierzonej zmianie z możliwością sprzeciwu ([§ RODO art. 28 ust. 2](#)), niezależnie od istotności podwykonawcy.
5. **Wpis do rejestru** w ciągu 10 dni roboczych od decyzji, z datą notyfikacji klienta.
6. **Dostęp** nadawany według [→ L3-DDS-04 · Procedura Zarządzania Dostępem](#) dopiero po wpisie i, gdy wymagane, po upływie terminu notyfikacji.

5. Wymagania przenoszone na podwykonawcę istotnego

OBSZAR	WYMAGANIE W UMOWIE Z PODWYKONAWCĄ	PO CO
Bezpieczeństwo i lokalizacje	Standardy bezpieczeństwa nie słabsze niż w → L1-DDS-01 ; uzgodnione lokalizacje danych; powiadomienie o ich zmianie.	Dostawca dotrzymuje zobowiązań z § DORA art. 30.2 lit. b i § DORA art. 30.2 lit. c .
Incydenty	Powiadomienie Dostawcy o incydencie z wpływem na usługę w terminie krótszym niż termin Dostawcy wobec klienta.	Dostawca zdąży powiadomić klienta (→ L3-DDS-02).
Zmiany i dalsze podwykonawstwo	Powiadomienie o własnych zmianach istotnych z wyprzedzeniem dłuższym niż termin notyfikacji wobec klienta.	Dostawca dotrzyma terminu z → L3-DDS-05 .
Audyt i dostęp	Prawo audytu i dostępu Dostawcy, klienta i jego organu nadzoru, bezpośrednio lub przez Dostawcę; dla dużych dostawców chmury akceptacja ich raportów niezależnych i programów audytowych.	Rozporządzenie delegowane (UE) 2025/532, art. 4: umowa określa warunki podwykonawstwa, w tym monitorowanie łańcucha i prawa dostępu i audytu wobec podwykonawców istotnych; wykonanie § DORA art. 30.3 lit. e .
Ciągłość	Plan ciągłości i testy właściwe dla usługi.	§ DORA art. 30.3 lit. c .
Wyjście i dane	Zwrot i usunięcie danych, wsparcie przy zmianie podwykonawcy.	Dostawca wesprze wyjście klienta (→ L3-DDS-09).
Współpraca z organami	Współpraca z organem nadzoru klienta.	§ DORA art. 30.2 lit. g .

DUZI DOSTAWCY CHMURY

Z dostawcą chmury publicznej nie wynegocjujesz indywidualnej umowy. Sprawdź, czy jego standardowe warunki i dodatek dotyczący usług finansowych (wielu dostawców publikuje dodatki DORA) pokrywają wymagania z tabeli, zapisz wynik w rejestrze i prześlij klientowi odniesienie do tych dokumentów.

6. Pola rejestru i przykładowe wpisy

POLE	ZAWARTOŚĆ
ID	POD-NN
Nazwa, kraj siedziby, identyfikator	Pełna nazwa; kraj; LEI, a gdy go brak, inny identyfikator wymagany przez klienta
Ranga i nadrzędny podmiot	2, 3...; od kogo zależy (dla rangi 3 i dalej)
Zakres usługi	Co wykonuje; ID usług z → A-DDS-06
Lokalizacje	Kraje świadczenia oraz przetwarzania i przechowywania danych
Istotność	PW1-PW5 spełnione; istotny tak / nie
Dane klienta	Dostęp tak / nie; podpowierzenie danych osobowych tak / nie
Ocena i dowody	Data oceny; certyfikaty lub raporty z datą ważności
Przeniesienie wymagań	Kompletne / częściowe (czego brak) / nie dotyczy
Notyfikacja klientów	Data notyfikacji, odpowiedź klienta
Alternatywa	Czy i jak można go zastąpić; szacowany czas
Przegląd	Data ostatniego i następnego przeglądu (co 12 miesięcy)

POLE	POD-01	POD-02	POD-03
Nazwa i ranga	Dostawca chmury publicznej (ranga 2)	Operator centrum danych dostawcy chmury (ranga 3, nadrzędny POD-01)	Zewnętrzny programista B2B (ranga 2)
Zakres	Hosting produkcji i kopii USL-01, USL-02	Infrastruktura fizyczna regionu chmury	Rozwój modułu raportów USL-02
Lokalizacje	Niemcy, Holandia	Niemcy	Polska; brak dostępu do produkcji
Istotność	PW1, PW2, PW3, PW4: istotny	PW3: istotny	brak kryteriów: nieistotny
Przeniesienie wymagań	Warunki standardowe + dodatek DORA dostawcy;	Przez POD-01 (raporty niezależne)	Umowa B2B z poufnością; nie

POLE	POD-01	POD-02	POD-03
	zweryfikowane 2026-08-10		dotyczy
Alternatywa	Inny region tego samego dostawcy; migracja do innej chmury ok. 6 miesięcy	Inny region POD-01	Zastępowalny w 2 tygodnie

7. Przegląd i dowody

- Przegląd podwykonawców istotnych co 12 miesięcy: aktualność certyfikatów i raportów, lokalizacje, incydenty, zmiany.
- Przegląd doraźny po incydencie u podwykonawcy, utracie jego certyfikatu lub zmianie jego właściciela.
- Dowody dla klienta: wyciąg z rejestru w formacie potrzebnym do jego rejestru informacji, umowy lub warunki z wymaganiami z rozdziału 5, kopie notyfikacji zmian.

8. Dostosowanie i zatwierdzenie

Dokument jest wzorem. Przed zatwierdzeniem uzupełnij pola oznaczone nawiasem kwadratowym, usuń przykłady, które nie dotyczą Twojej organizacji, i sprawdź, czy wartości (terminy, częstotliwości) są zgodne z umowami zawartymi z klientami. Gdy umowa z klientem przewiduje termin ostrzejszy niż ten dokument, obowiązuje termin z umowy.

- Wpisz wszystkich podwykonawców usług z [→ A-DDS-06 · Rejestr Aktywów i Usług ICT](#), także dostawców chmury, centrów danych, narzędzi z dostępem do danych klientów i zewnętrznych programistów (B2B, software house).
- Identyfikatory podwykonawców (LEI lub inny wymagany przez klienta) uzupełnij przed pierwszym zapytaniem klienta o dane do rejestru informacji.
- Przykładowe wpisy (rozdział 6) usuń po założeniu rejestru.

CZYNNOŚĆ	IMIĘ I NAZWISKO	DATA	PODPIS
Opracował	[IMIĘ I NAZWISKO]	[DATA]	
Zatwierdził (Zarząd)	[IMIĘ I NAZWISKO]	[DATA ZATWIERDZENIA]	

CHARAKTER DOKUMENTU

Wzór dokumentacji opracowany przez RealSec dla dostawców usług ICT obsługujących podmioty finansowe. Nie stanowi porady prawnej, audytu ani oceny zgodności i nie gwarantuje pozytywnego wyniku oceny dostawcy przez klienta ani organ nadzoru. Za dostosowanie, wdrożenie i stosowanie dokumentu odpowiada organizacja, która go przyjmuje.

9. Historia zmian

WERSJA	DATA	AUTOR	OPIS ZMIANY
v1.0	2026-10-02	RealSec (wzór)	Wydanie wzoru w pakiecie Dostawca DORA Start.
[WERSJA]	[DATA]	[IMIĘ I NAZWISKO]	Dostosowanie do [NAZWA DOSTAWCY] i zatwierdzenie przez Zarząd.

PRÓBKA