DORA dla dostawców IT – checklista

Co bank sprawdza, zanim podpisze umowę na IT staff augmentation (body leasing)

Commoditech
commoditech.pl

DORA – rozporządzenie (UE) 2022/2554 – stosuje się od 17 stycznia 2025 r. Rozdział V, sekcja I (art. 28–30) określa, co podmiot finansowy musi ocenić przed zawarciem i w trakcie umowy z zewnętrznym dostawcą usług ICT. Szczegóły doprecyzowują: rozporządzenie delegowane (UE) 2024/1773 (polityka umowna dla usług wspierających funkcje krytyczne lub istotne), rozporządzenie wykonawcze (UE) 2024/2956 (wzory rejestru informacji) i rozporządzenie delegowane (UE) 2025/532 (podwykonawstwo). Czy dana usługa body leasingu jest usługą ICT (art. 3 pkt 21) i czy wspiera funkcję krytyczną lub istotną – ocenia bank. Poniżej lista pytań dla działów zarządzania dostawcami w bankach i dla dostawców IT, którzy chcą być na nie przygotowani – z podstawą prawną i wskazaniem, jakich dokumentów lub zobowiązań oczekiwać.

	Co sprawdza bank	Podstawa	O co poprosić dostawcę / co przygotować
A.	**Przed umową – ocena i należyta staranność**		
☐	**Czy usługa wspiera funkcję krytyczną lub istotną?**	art. 28 ust. 4 lit. a; art. 3 pkt 22	Opis ról, zakresu prac i systemów, do których specjaliści dostawcy będą mieli dostęp – podstawa klasyfikacji, którą przeprowadza bank.
☐	**Dane dostawcy do rejestru informacji**	art. 28 ust. 3; rozp. wyk. 2024/2956	Pełna nazwa, adres, KRS, NIP, REGON i kod LEI (jeśli dostawca nie ma LEI – termin jego uzyskania przed podpisaniem umowy).
☐	**Należyta staranność i sytuacja dostawcy**	art. 28 ust. 4 lit. d; rozp. del. 2024/1773 art. 6	Odpis z KRS, struktura własności, sprawozdania finansowe (publicznie w KRS lub na żądanie), referencje od klientów.
☐	**Konflikty interesów**	art. 28 ust. 4 lit. e; rozp. del. 2024/1773 art. 7	Zasady, które wykluczają równoległą pracę konsultanta dla konkurenta banku w tym samym obszarze, oraz sposób ich egzekwowania.
☐	**Ryzyko koncentracji i zastępowalność dostawcy**	art. 29 ust. 1	Skala dostawcy (liczba specjalistów w aktywnych umowach), źródła pozyskiwania zastępców, czas obsadzenia roli zastępczej.
☐	**Standardy bezpieczeństwa informacji**	art. 28 ust. 5	W czyim środowisku pracują specjaliści (sprzęt, VPN/VDI banku czy dostawcy), posiadane certyfikaty (np. ISO/IEC 27001) lub opis stosowanych zabezpieczeń.
B.	**Umowa – postanowienia minimalne (art. 30 ust. 2)**		
☐	**Opis usług i warunki podwykonawstwa**	art. 30 ust. 2 lit. a; rozp. del. 2025/532	Czy dostawca korzysta z podwykonawców – w tym kontraktorów B2B – oraz czy ujawnia ich bankowi i przenosi na nich obowiązki dotyczące bezpieczeństwa, poufności i audytu.
☐	**Miejsca świadczenia usług i przetwarzania danych**	art. 30 ust. 2 lit. b	Kraje i lokalizacje, z których pracują specjaliści, oraz miejsca przetwarzania danych banku.
☐	**Poufność, integralność i ochrona danych osobowych**	art. 30 ust. 2 lit. c	Umowa ramowa z NDA i klauzulami RODO; NDA i oświadczenie o tajemnicy bankowej (art. 104 Prawa bankowego) podpisywane przez każdego konsultanta.
☐	**Dostęp, odzyskanie i zwrot danych po zakończeniu**	art. 30 ust. 2 lit. d	Zobowiązanie do zwrotu lub trwałego usunięcia danych i odwołania dostępów po zakończeniu współpracy, z pisemnym potwierdzeniem; przeniesienie praw do rezultatów prac.
☐	**Poziomy usług (SLA)**	art. 30 ust. 2 lit. e; ust. 3 lit. a	Czas reakcji na zapotrzebowanie, czas przedstawienia profili, czas zastępstwa, zasady przekazania wiedzy i ich koszt.
☐	**Pomoc przy incydencie ICT**	art. 30 ust. 2 lit. f	Procedura zgłaszania incydentów z konkretnym czasem powiadomienia banku (w godzinach) i rejestrem zdarzeń.
☐	**Współpraca z organami nadzoru**	art. 30 ust. 2 lit. g	Zobowiązanie do pełnej współpracy z organami nadzoru (np. KNF, EBC) i audytorami działającymi w imieniu banku.
☐	**Prawo wypowiedzenia i okresy wypowiedzenia**	art. 28 ust. 7; art. 30 ust. 2 lit. h	Przesłanki wypowiedzenia z art. 28 ust. 7 w umowie; okresy wypowiedzenia u dostawcy i jego konsultantów – czas na wdrożenie następcy.
☐	**Udział w szkoleniach z bezpieczeństwa ICT**	art. 30 ust. 2 lit. i; art. 13 ust. 6	Zobowiązanie do udziału specjalistów w szkoleniach z bezpieczeństwa ICT organizowanych przez bank.
C.	**Funkcje krytyczne lub istotne – wymogi dodatkowe (art. 30 ust. 3)**		
☐	**Raportowanie istotnych zmian u dostawcy**	art. 30 ust. 3 lit. b	Zobowiązanie do informowania banku bez zbędnej zwłoki o zmianach własności, kluczowego personelu i podwykonawców.
☐	**Plany awaryjne i ich testowanie**	art. 30 ust. 3 lit. c	Plan ciągłości działania z datą przyjęcia, datą ostatniego lub planowanego testu i rejestrem testów.
☐	**Udział w testach TLPT**	art. 30 ust. 3 lit. d; art. 26–27	Zobowiązanie do współpracy w testach bezpieczeństwa ICT / TLPT banku w zakresie wymaganym umową.
☐	**Nieograniczone prawo dostępu, kontroli i audytu**	art. 30 ust. 3 lit. e; art. 28 ust. 6	Prawo audytu i kontroli dla banku, jego audytorów i organów nadzoru; dostęp do dokumentacji i personelu realizującego umowę.
☐	**Strategia wyjścia i okres przejściowy**	art. 28 ust. 8; art. 30 ust. 3 lit. f; rozp. del. 2024/1773 art. 10	Plan wyjścia: okres przejściowy, sposób prowadzenia dokumentacji, protokół przekazania wiedzy, zwrot danych i dostępów.

Dwa pojęcia, od których zależy zakres wymogów

Usługi ICT (art. 3 pkt 21): *„usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego […]”*

Krytyczna lub istotna funkcja (art. 3 pkt 22): *„funkcja, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu […]”*

Jeżeli bank uzna, że specjaliści dostawcy wspierają funkcję krytyczną lub istotną, obowiązuje cała część C checklisty, a umowa trafia do rejestru informacji z odpowiednim oznaczeniem (art. 28 ust. 3).

Pakiet dokumentów, który dostawca powinien mieć gotowy

☐	Odpis z KRS i dane do rejestru informacji (w tym kod LEI)
☐	Wzór umowy ramowej z postanowieniami z art. 30 ust. 2 (i ust. 3 dla funkcji krytycznych lub istotnych)
☐	Wzór NDA i oświadczenia o tajemnicy bankowej dla konsultanta
☐	Zasady podwykonawstwa – w tym status kontraktorów B2B w łańcuchu dostaw
☐	Lista miejsc świadczenia usług i przetwarzania danych
☐	Procedura obsługi i zgłaszania incydentów ICT z czasem powiadomienia
☐	Plan ciągłości działania z datą ostatniego testu
☐	Plan wyjścia: okres przejściowy, przekazanie wiedzy, zwrot danych i dostępów
☐	Opis SLA: czas reakcji, czas przedstawienia profili, zastępstwo
☐	Polisa OC (suma gwarancyjna, okres ubezpieczenia)

Poza DORA, ale zwykle w RFP banku

Polisa OC (suma gwarancyjna, okres ubezpieczenia, zakres obejmujący usługi IT), certyfikaty bezpieczeństwa – jeśli dostawca je posiada, referencje od klientów z sektora finansowego, dokumenty finansowe.

Akty prawne (wersje polskie, EUR-Lex)

Rozporządzenie (UE) 2022/2554 (DORA), art. 28–30 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022R2554

Rozporządzenie delegowane Komisji (UE) 2024/1773 – polityka umowna (RTS) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1773

Rozporządzenie wykonawcze Komisji (UE) 2024/2956 – rejestr informacji (ITS) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2956

Rozporządzenie delegowane Komisji (UE) 2025/532 – podwykonawstwo (RTS) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32025R0532

Jak korzystać: zaznacz ☐ przy punktach, które dostawca udokumentował. Brak odpowiedzi w części C przy usłudze wspierającej funkcję krytyczną lub istotną zwykle zatrzymuje podpisanie umowy.

Chcesz porównać tę listę z dokumentacją, którą macie od obecnych dostawców? Commoditech Sp. z o.o., al. KEN 15/48, 02-797 Warszawa · konrad.wojtasik@commoditech.pl · +48 791 662 241 · commoditech.pl