ZEWNĘTRZNY DZIAŁ BEZPIECZEŃSTWA PUSHSEC. OPIS ROLI, POZIOM 1 Z 3

Specjalista ds. bezpieczeństwa informacji jako usługa

Twój system bezpieczeństwa ma **dowód działania co miesiąc**: aktualne dokumenty, wykonane przeglądy z zapisem, gotowy pakiet na audyt i kwestionariusz. Bez etatu, od 3 dni w miesiącu.

Poziom 1. Specjalista	Poziom 2. Manager i Pełnomocnik ds. SZBI	Poziom 3. vCISO

1 600 zł	**3 / 6 / 10 dni**	**2 godziny**	**od 3 mies.**
stała dniówka netto	wymiar do wyboru	pierwsza odpowiedź w dni robocze	umowa, bez kar umownych

1. Co dostajesz

Rola jest rozliczana z produktów, nie z obecności. Każda pozycja ma nazwę, częstotliwość i odbiorcę; w pełnym wymiarze dostajesz wszystkie.

Notatka statusowa

Jedna strona co miesiąc: zrobione, otwarte, ryzyka, decyzje potrzebne od Ciebie, ewidencja dni per obszar.

Miesięcznie. Kierownik IT, Zarząd

Rejestr zapisów SZBI

Jedno miejsce, z którego widać, że system działa: każde działanie cykliczne z częstotliwością, właścicielem, datą i linkiem do dowodu.

Prowadzony stale. Audytor, Pełnomocnik

Protokoły przeglądów

Przegląd uprawnień, kopii zapasowych, dostawców i zgodności z politykami, każdy z listą działań i terminami.

Po każdym przeglądzie. Repozytorium SZBI

Pakiet dowodowy na audyt

Dowody ułożone według listy wymagań audytora lub klienta, z listą braków i planem domknięcia. Zero szukania w dniu audytu.

Przed audytem lub kontrolą. Audytor, klient

Komplet odpowiedzi na kwestionariusz

Odpowiedzi w formacie kontrahenta, zgodne ze stanem faktycznym, z listą pozycji do Twojej decyzji i aktualizacją biblioteki odpowiedzi.

Zdarzeniowo. Zarząd, dział sprzedaży

Szkolenie z zaświadczeniami

Szkolenie wstępne dla nowych osób i roczne dla zespołu: materiały, test, lista obecności, zaświadczenia.

Rocznie i przy zatrudnieniu. HR, audytor

Dla kogo ten poziom

- Firmy 20 do 150 osób zaczynające pracę z compliance, bez etatu bezpieczeństwa.
- Organizacje po health-checku dokumentacji SZBI, które chcą domknąć ustalenia i utrzymać porządek.
- Firmy z certyfikatem ISO 27001, w których Pełnomocnik ma inne obowiązki i brakuje rąk do pracy operacyjnej.
- Kancelarie prawne i LegalTech, gdzie bezpieczeństwem zajmuje się ktoś przy okazji.

Sytuacja wyjściowa, z którą przychodzą klienci

- Polityki istnieją, ale ostatnia aktualizacja była przy wdrożeniu.
- Przegląd uprawnień wykonywany przy odejściach, bez utrwalenia wyniku.
- Klient enterprise przysłał kwestionariusz i nie ma komu go oddać.
- Za pół roku audyt nadzoru, a katalog Zapisy jest pusty.

2. Wymiar współpracy: 10 dni albo mniej

Pełny wymiar to 10 dni roboczych w miesiącu. Mniejszy wymiar nie oznacza gorszej jakości, tylko węższy zakres: część obszarów przechodzi w tryb ograniczony albo poza wymiar. Dniówka jest stała dla poziomu, więc płacisz za dni, a nie za etykietę.

Podstawowy

3 dni

4 800 zł netto / mies.

Firmy do 30 osób z gotową dokumentacją. Utrzymanie zapisów i dyżur dla IT.

Standard

6 dni

9 600 zł netto / mies.

Firmy 30 do 100 osób lub przed audytem nadzoru. Pełne przeglądy i kwestionariusze.

Pełny Pełny wymiar

10 dni

16 000 zł netto / mies.

Firmy 100 do 150 osób, po health-checku z wieloma ustaleniami, z częstymi kwestionariuszami.

Obszar	Podstawowy (3 dni)	Standard (6 dni)	Pełny (10 dni)
Notatka statusowa i dyżur pytań dla IT (odpowiedź do 2 godzin)	✔	✔	✔
Rejestr zapisów SZBI i rejestry: aktywa, dostawcy, incydenty, szkolenia	◔	✔	✔
Przeglądy cykliczne z protokołem: uprawnienia, kopie zapasowe, dostawcy, polityki	◔	✔	✔
Utrzymanie polityk i procedur, przeglądy roczne, aktualizacja odwołań	◔	✔	✔
Pakiet dowodowy na audyt i wsparcie podczas audytu	·	◔	✔
Kwestionariusze bezpieczeństwa od klientów	·	◔	✔
Szkolenia świadomościowe z testem i zaświadczeniami	·	◔	✔
Checklisty i konsultacje dla IT: onboarding, offboarding, zmiany, konfiguracja bazowa	·	◔	✔
Domykanie ustaleń z health-checku lub audytu (praca własna, nie tylko nadzór)	·	·	✔
Wsparcie w obsłudze incydentu: fakty, rejestr, notatka po incydencie	·	◔	✔

✔ w pełnym zakresie ◔ w ograniczonym zakresie (opisany w umowie) · poza wymiarem, dostępne jako projekt w stałej cenie

3. Przykładowy miesiąc w pełnym wymiarze

Tak wygląda typowy miesiąc w utrzymaniu, po pierwszych 90 dniach. Dni są przesuwane między obszarami zależnie od tego, co się dzieje (audyt, incydent, kwestionariusz); ewidencja dni jest w raporcie miesięcznym.

Dzień	Obszar	Co powstaje
1	Spotkanie statusowe i plan miesiąca	Agenda z priorytetami, aktualizacja planu działania, lista decyzji dla Kierownika IT
2	Przegląd uprawnień (w miesiącu, na który przypada) lub przegląd dostawców	Protokół z listą kont do zamknięcia lub dostawców do aktualizacji, terminy
3	Weryfikacja kopii zapasowych i odtworzenia	Zapis z testu odtworzenia, wynik, uwagi dla IT
4	Dokumentacja	Aktualizacja 2 do 3 dokumentów z terminem przeglądu, rejestr informacji udokumentowanej
5	Rejestry	Aktualizacja rejestru aktywów, dostawców, incydentów; uzupełnienie rejestru zapisów
6	Kwestionariusz od klienta lub domykanie ustaleń	Komplet odpowiedzi do zatwierdzenia albo 2 ustalenia z health-checku domknięte z dowodem
7	Wsparcie IT	Konsultacje przy zmianach, checklista onboardingu i offboardingu, notatka z konsultacji
8	Szkolenie lub pakiet dowodowy	Szkolenie wstępne dla nowych osób z listą i testem, albo dowody ułożone pod nadchodzący audyt
9	Przegląd zgodności z jedną polityką	Protokół: co jest stosowane, co nie, działania
10	Zamknięcie miesiąca	Notatka statusowa, ewidencja dni, lista tematów na kolejny miesiąc, rezerwa na pytania

4. Fragment produktu, który dostajesz co miesiąc

Notatka statusowa SZBI. Sierpień 2026 FRAGMENT PRZYKŁADOWY

Demo SaaS Sp. z o.o. Specjalista ds. bezpieczeństwa informacji, PushSec. Wymiar: 6 dni

Zrobione

- Przegląd uprawnień H2: 41 kont, 6 do zamknięcia, zamknięte 28.08. Protokół PU-2026-02.
- Test odtworzenia kopii bazy produkcyjnej: 42 min, zgodnie z RPO. Zapis KZ-2026-08.
- Polityka kontroli dostępu v2.1: odwołania do ISO 27001:2022, zatwierdzona 20.08.
- Kwestionariusz kontrahenta FinCo: 128 pytań, komplet do zatwierdzenia 31.08.

Otwarte

- Inwentarz aktywów: 3 usługi SaaS działu marketingu bez właściciela. Termin 15.09, właściciel: Dyrektor Operacyjny.
- Szkolenie wstępne dla 2 nowych osób: zaplanowane 05.09.

Ryzyko

- Umowa z dostawcą hostingu bez klauzuli o zgłaszaniu incydentów. Rekomendacja: aneks przy odnowieniu w październiku.

Decyzje potrzebne od Ciebie

- Zgoda na wysyłkę kwestionariusza FinCo, w tym 2 pozycje tworzące zobowiązanie umowne (prawo audytu, suma polisy).

Zapis w tym miesiącu	Data	Dowód	Następny termin
Przegląd uprawnień	26.08.2026	PU-2026-02, repozytorium SZBI/Zapisy/Dostęp	02.2027
Test odtworzenia kopii	19.08.2026	KZ-2026-08	09.2026
Przegląd dostawców krytycznych	12.08.2026	PD-2026-Q3	11.2026

Ewidencja dni: dokumentacja 1,5, przeglądy 2, kwestionariusz 1,5, wsparcie IT 0,5, zamknięcie miesiąca 0,5. Razem 6 z 6.

5. Pierwsze 90 dni

Pierwszy miesiąc zawsze kończy się planem działania, który zostaje u Ciebie, niezależnie od tego, czy kontynuujemy.

Miesiąc 1. Diagnoza

- Inwentaryzacja dokumentacji i rejestrów, sprawdzenie, co jest, co jest nieaktualne, czego brakuje.
- Uruchomienie rejestru zapisów SZBI z częstotliwościami i właścicielami.
- Plan działania na 12 miesięcy zatwierdzony przez Kierownika IT i Zarząd.

Miesiąc 2. Uruchomienie

- Wykonanie zaległych przeglądów: uprawnienia, kopie, dostawcy, z protokołami.
- Aktualizacja polityk z nieaktualnymi odwołaniami do normy.
- Ustalenie rytmu: dyżur, spotkanie statusowe, kanał zgłoszeń dla IT.

Miesiąc 3. Pierwszy pełny cykl

- Pierwsze szkolenie świadomościowe z listą obecności i testem.
- Komplet zapisów za pierwszy zamknięty miesiąc w repozytorium.
- Przegląd kwartalny i decyzja, czy poziom 1 nadal pasuje do skali organizacji.

6. Rola w skrócie

Poziom w drabince	1 z 3. Najprostsza ścieżka wejścia do zewnętrznego działu bezpieczeństwa.
Charakter roli	Operacyjna. Wykonuje pracę przy SZBI, nie podejmuje decyzji o ryzyku i nie reprezentuje organizacji na zewnątrz.
Komu raportuje	Kierownikowi IT lub osobie wskazanej przez Zarząd jako właściciel SZBI po stronie klienta.
Formalne funkcje	Brak formalnego umocowania w organizacji klienta. Rola nie zastępuje Pełnomocnika ds. SZBI (poziom 2).
Wymiar	3, 6 lub 10 dni roboczych miesięcznie, w tym spotkanie statusowe i dyżur pytań dla IT.
Cena	Stała dniówka 1 600 zł netto: 4 800, 9 600 lub 16 000 zł miesięcznie zależnie od wymiaru.
Kto pełni rolę	Konsultant PushSec z doświadczeniem w prowadzeniu SZBI, pod nadzorem merytorycznym ISO/IEC 27001 Lead Auditora.
Główne ramy odniesienia	ISO/IEC 27001:2022 z Załącznikiem A, wewnętrzne polityki klienta, wymagania kontraktowe klientów końcowych.

7. Zakres odpowiedzialności i co pokrywa

Kolumna Wymaganie pokazuje, które obowiązki z normy lub przepisu dana pozycja pokrywa. Kolumna Dowód pokazuje zapis, którym wykażesz to audytorowi, klientowi albo organowi.

Obszar	Zadania w tej roli	Wymaganie	Dowód
Dokumentacja SZBI	Utrzymanie polityk, procedur i instrukcji: wersjonowanie, przeglądy roczne, aktualizacja odwołań do normy i przepisów, rejestr informacji udokumentowanej.	ISO 27001 pkt 7.5; kontrole A.5.1, A.5.37	Aktualna dokumentacja z historią zmian, rejestr dokumentów z datą następnego przeglądu
Rejestry i zapisy	Prowadzenie rejestru aktywów, rejestru dostawców, rejestru incydentów, rejestru szkoleń oraz rejestru zapisów SZBI (co, jak często, gdzie dowód).	ISO 27001 pkt 7.5.3, 9.1; A.5.9, A.5.19, A.5.24, A.6.3	Rejestry z datami i właścicielami, rejestr zapisów SZBI

Obszar	Zadania w tej roli	Wymaganie	Dowód
Przeglądy cykliczne	Przegląd uprawnień, weryfikacja kopii zapasowych i odtworzeń, przegląd alertów w ujęciu organizacyjnym, przegląd dostawców, przegląd zgodności z politykami.	A.5.18, A.8.13, A.8.15, A.8.16, A.5.22	Protokół z każdego przeglądu, lista działań z terminami
Wsparcie działu IT	Konsultacje przy zmianach w środowisku, checklisty onboardingu i offboardingu, wytyczne konfiguracji bazowej, weryfikacja spełnienia polityk przy nowych systemach.	A.5.16, A.6.5, A.8.9, A.8.32	Uzgodnione checklisty, notatki z konsultacji, lista otwartych tematów
Przygotowanie do audytów i kontroli	Kompletowanie dowodów wg listy audytora, uporządkowanie repozytorium, udział w audycie jako osoba prezentująca dokumentację, obsługa próśb o dowody od klientów.	ISO 27001 pkt 9.2 (wsparcie), 9.3 (dane wejściowe)	Pakiet dowodowy, lista braków z planem domknięcia
Kwestionariusze bezpieczeństwa od klientów	Odpowiedzi na podstawie biblioteki odpowiedzi organizacji, zgodne ze stanem faktycznym. Pozycje tworzące zobowiązania umowne przekazywane do decyzji Zarządu.	A.5.19, A.5.20; wymagania kontraktowe	Komplet odpowiedzi do zatwierdzenia, aktualizacja biblioteki odpowiedzi
Szkolenia świadomościowe	Szkolenie wstępne dla nowych osób i szkolenie roczne dla zespołu, test wiedzy, lista obecności, zaświadczenia.	ISO 27001 pkt 7.2, 7.3; A.6.3; UoKSC art. 8 ust. 1 (jeśli podmiot objęty)	Materiały, rejestr uczestników, wyniki testu
Incydenty, poziom operacyjny	Prowadzenie rejestru zdarzeń, wsparcie w zebraniu faktów, notatka po incydencie i wnioski. Klasyfikacja i decyzje o zgłoszeniach zewnętrznych należą do poziomu 2 lub Zarządu.	A.5.24 do A.5.28	Rejestr incydentów, notatka post-incydentowa

8. Z czego rozliczamy rolę

Miernik	Wartość docelowa	Skąd dane
Przeglądy cykliczne wykonane w terminie z zapisem	100%	Rejestr zapisów SZBI
Dokumenty po terminie przeglądu	0	Rejestr informacji udokumentowanej
Czas pierwszej odpowiedzi na pytanie IT	do 2 godzin w dni robocze	Kanał zgłoszeń, notatka statusowa
Nowi pracownicy przeszkoleni w ciągu 30 dni od zatrudnienia	95% i więcej	Rejestr szkoleń
Dowody nieodnalezione podczas audytu	0	Raport z audytu, lista braków
Działania z planu zamknięte w terminie	80% i więcej kwartalnie	Plan działania

9. Granice roli i sygnały, że potrzebujesz więcej

Poza zakresem tej roli	Gdzie to jest
Formalna funkcja Pełnomocnika ds. SZBI i osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa	Poziom 2, Manager
Kontakt z jednostką certyfikującą, audytorami klientów i regulatorem	Poziom 2 i 3
Decyzje o akceptacji ryzyka i o zgłoszeniu incydentu do organów	Zarząd, z rekomendacją poziomu 2
Raportowanie do Zarządu i nadzór nad planem postępowania z ryzykiem	Poziom 2, Manager
Audyt wewnętrzny SZBI	Odrębna usługa, inny audytor ze względu na bezstronność (ISO 27001 pkt 9.2)
Testy penetracyjne, administrowanie systemami, monitoring SOC	Dział IT klienta lub partner techniczny
Funkcja Inspektora Ochrony Danych	Odrębna rola
Strategia, budżet bezpieczeństwa, reprezentacja przed KNF i inwestorami	Poziom 3, vCISO

Sygnały, że czas na poziom 2 (Manager)

- Certyfikacja ISO 27001 w horyzoncie 12 miesięcy: norma wymaga osoby z odpowiedzialnością za SZBI i raportowaniem do kierownictwa (pkt 5.3).
- Wpis do wykazu podmiotów kluczowych lub ważnych na gruncie UoKSC albo wymagania KNF.
- Klient enterprise lub audytor kontrahenta oczekuje jednej osoby odpowiedzialnej za bezpieczeństwo, nie wykonawcy zadań.
- Zarząd chce otrzymywać regularne raporty o stanie bezpieczeństwa i ryzykach.
- Rejestr ryzyka wymaga prowadzenia z właścicielami i akceptacją ryzyk rezydualnych.

Czego potrzebujemy po Twojej stronie

- Sponsor po stronie Zarządu i jedna osoba kontaktowa w IT z decyzyjnością operacyjną.
- Dostęp do repozytorium dokumentacji SZBI i do narzędzi, w których powstają zapisy (system ticketowy, panel IdP w trybie odczytu, backup).
- Około 2 do 3 godzin miesięcznie czasu kierownika IT na spotkanie statusowe i pytania.
- Lista pracowników i dostawców na start oraz informacja o planowanych audytach i kwestionariuszach.

10. Koszt tej funkcji na etacie i najczęstsze pytania

14 000 do 26 000 zł/mc

Specjalista GRC na etacie: 12 do 22 tys. brutto plus ok. 20% kosztów pracodawcy, do tego 2 do 3 miesięcy rekrutacji, wdrożenie, urlopy i ryzyko rotacji. Etat kupuje się w całości, nawet gdy pracy jest na 3 dni.

4 800 do 16 000 zł/mc

Ta rola jako usługa: 3, 6 lub 10 dni. Płacisz za dni, których realnie potrzebujesz, start w kilka dni, ciągłość zapisana w umowie.

Nadzór w cenie

Każdy dzień pracy jest pod nadzorem Lead Auditora z doświadczeniem z audytów certyfikujących. Na etacie tej kontroli jakości nie ma.

Czy 3 dni w miesiącu to nie za mało, żeby coś się zmieniło?
W 3 dniach utrzymujemy system, który już istnieje: zapisy, dyżur, podstawowe przeglądy. Jeśli dokumentacja wymaga porządkowania, pierwsze 3 miesiące robimy w wymiarze 6 lub 10 dni i schodzimy niżej, gdy zapisy się ustabilizują.

Co jeśli w danym miesiącu nie będzie pracy na 10 dni?
Dni niewykorzystane przechodzą na kolejny miesiąc w ramach kwartału, a wymiar można obniżyć od następnego kwartału. Ewidencję dni widzisz w każdej notatce statusowej.

Czy Specjalista może być naszym Pełnomocnikiem ds. SZBI?
Nie. Pełnomocnik wymaga formalnego umocowania i odpowiada za system jako całość. To poziom 2. Specjalista pracuje pod Pełnomocnikiem, także wtedy, gdy jest nim ktoś z Twojej organizacji.

Kto realnie wykonuje pracę?
Konsultant PushSec przypisany do Twojej organizacji na cały okres umowy, pod nadzorem merytorycznym Lead Auditora. Nie rotujemy osób między klientami bez uzgodnienia.

Dniówka 1 600 zł to więcej niż stawka seniora na B2B. Za co płacę różnicę?
Za to, czego kontraktor nie daje: nadzór merytoryczny Lead Auditora nad każdym produktem, zastępowalność osoby bez utraty kontekstu, gotowe narzędzia i szablony PushSec, OC zawodowe 1,5 mln zł oraz brak kosztu rekrutacji i wdrożenia. Płacisz za dni, nie za etat, więc przy 3 lub 6 dniach jesteś wyraźnie poniżej kosztu pracownika.

Co zostaje u nas, jeśli zakończymy współpracę po 3 miesiącach?
Plan działania, rejestr zapisów, wszystkie protokoły, zaktualizowane dokumenty i biblioteka odpowiedzi. Wszystko w Twoim repozytorium, nie u nas.

11. Warunki współpracy

Wymiar i cena	Stała dniówka dla poziomu, niezależna od wymiaru. Dni niewykorzystane w miesiącu przechodzą na kolejny miesiąc w ramach kwartału. Ewidencja dni per obszar w raporcie miesięcznym.
Umowa	Minimum 3 miesiące, potem miesięczne wypowiedzenie. Bez zobowiązania rocznego, bez kar umownych.
Zmiana wymiaru lub poziomu	Co kwartał decyzja o wymiarze (w górę lub w dół) i o poziomie drabinki. Bez zmiany dostawcy, z zachowaniem kontekstu.
Czas reakcji	Pierwsza odpowiedź do 2 godzin w dni robocze. Dla incydentów ścieżka uzgodniona na kickoffie.
Nadzór merytoryczny	Każdy poziom działa pod nadzorem certyfikowanego ISO/IEC 27001 Lead Auditora (BSI, IRCA). Standard pracy nie zależy od pojedynczej osoby.
Poufność i dane	NDA przed przekazaniem dokumentacji, umowa powierzenia, gdy zakres tego wymaga.
Własność wyników	Plan działania i cała wytworzona dokumentacja pozostają własnością klienta, także po zakończeniu umowy.
Ubezpieczenie	OC zawodowe konsultanta ds. bezpieczeństwa: 1,5 mln zł, w tym klauzula cyber i RODO 200 tys. zł (Lloyd's).
Forma pracy	Zdalnie lub hybrydowo. Warszawa i okolice: spotkania na miejscu w uzgodnionym rytmie.
Ceny	Netto, doliczamy 23% VAT.

12. Dowody

> *PushSec łączy podejście praktyczne z uwzględnieniem wymagań regulacyjnych. Dzięki współpracy poprawiliśmy poziom organizacji w obszarze bezpieczeństwa informacji, zgodności oraz odporności operacyjnej.*
>
> **Fincard, instytucja płatnicza. Wdrożenie DORA, model vCISO**

> *Firma jest rzetelnym partnerem merytorycznym i biznesowym, realizuje usługi z należytą starannością. Powierzone zadania są wykonywane w pełni profesjonalnie i z dbałością o jakość.*
>
> **DS Stream, firma technologiczna. Audyt i doradztwo ISO 27001**

> *Rafał Dobrosielski wykazał się rzetelnością, kompetencją, dbałością o klienta oraz szeroką znajomością tematyki bezpieczeństwa IT.*
>
> **NetCredit, firma finansowa. Szkolenia z cyberbezpieczeństwa**

Pełne listy referencyjne: pushsec.pl/klienci

Zobacz produkt, zanim zapłacisz

Publiczne próbki dokumentów w tym stylu i na tym poziomie szczegółowości, na dwóch fikcyjnych podmiotach: Demo SaaS Sp. z o.o., 45 osób (startery, poziomy 1 i 2) i Demo Platform Sp. z o.o., B2B SaaS 140 osób z klientami bankowymi (vCISO):

- Raport health-check dokumentacji SZBI (17 obszarów, karty ustaleń)
- Komplet odpowiedzi na kwestionariusz bezpieczeństwa z biblioteką odpowiedzi
- Raport samoidentyfikacji KSC
- Demo diagnozy startowej, raportu miesięcznego dla Zarządu i mapy drogowej 12M vCISO (pushsec.pl/vciso)

pushsec.pl/sklep

Kto za tym stoi

Rafał Dobrosielski, auditor wiodący ISO/IEC 27001 (BSI, IRCA), vCISO. Wdrożenia DORA, ISO 27001 i NIS2/KSC w FinTech, SaaS i kancelariach. Autorska metodyka health-check: 17 obszarów SZBI, 157 punktów kontrolnych. OC zawodowe 1,5 mln zł.

Następny krok: 30 minut, po których dostajesz ofertę w dwóch wariantach

Na bezpłatnej konsultacji ustalamy poziom i wymiar. Po rozmowie otrzymujesz ofertę z wariantem wejściowym i docelowym, z cenami i zakresem per obszar. Małe kupuje się łatwo, dlatego zawsze pokazujemy prostszą ścieżkę.

pushsec.pl/kontakt/?temat=specjalista · info@pushsec.pl · (+48) 780 519 553 · Wszystkie poziomy i widełki: pushsec.pl/vciso

Skróty: ISO 27001 oznacza normę ISO/IEC 27001:2022. UoKSC oznacza ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20, ze zm. Dz.U. 2026 poz. 252). DORA oznacza rozporządzenie (UE) 2022/2554. RODO oznacza rozporządzenie (UE) 2016/679. Odwołania do wymagań pokazują, które obowiązki rola pokrywa; nie stanowią opinii prawnej. Fragmenty dokumentów w tym opisie dotyczą fikcyjnych podmiotów Demo SaaS Sp. z o.o. i Demo Platform Sp. z o.o.