					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII23					Tytuł dokumentu: **Polityka podmiotu przetwarzającego PII w chmurze obliczeniowej**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Applicability	Coverage Type	Komentarz
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Rola PIMS i stosowalność zabezpieczeń
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Udokumentowane dowody dotyczące podmiotu przetwarzającego w chmurze obliczeniowej i kontrola operacyjna
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitorowanie, niezgodność i działanie korygujące
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Umowy z klientami, polecenia, wsparcie i zapisy
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Wsparcie klienta w zakresie obowiązków wobec osoby, której dane dotyczą
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Pliki tymczasowe, zwrot, transfer, utylizacja i środki kontroli transmisji
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Podstawa i lokalizacje transferu
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Zapisy ujawnień i obsługa wniosków o ujawnienie
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Ujawnianie podwykonawców, angażowanie i powiadomienie o zmianie
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Dostęp, zapisy, kopie zapasowe i dowody rejestrowania

GDPR	Article 28	Processor	Primary	Podmiot przetwarzający, podwykonawca przetwarzania, wsparcie, audyt, usunięcie i zwrot
GDPR	Article 30	Processor	Supporting	Zapisy podmiotu przetwarzającego
GDPR	Article 32; Article 33	Processor	Supporting	Bezpieczeństwo i powiadomienie administratora o naruszeniu
GDPR	Article 44	Conditional	Referenced	Ścieżka międzynarodowego transferu
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Cel, minimalizacja, wykorzystanie, okres przechowywania i ograniczenie ujawniania
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Rozliczalność, bezpieczeństwo informacji i zgodność
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Ocena podmiotu przetwarzającego, monitorowanie, zmiana i środki kontroli okresu przechowywania
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Stosowalność zabezpieczeń, kontrola operacyjna oraz środki kontroli dostawców i chmury obliczeniowej
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Środki kontroli dostawców, chmury obliczeniowej, usuwania, rejestrowania i monitorowania
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Wsparcie klienta przez podmiot

				przetwarzający w chmurze obliczeniowej i ograniczenie celu
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Powiadomienia o ujawnieniach w chmurze obliczeniowej, zapisy ujawnień i przejrzystość podwykonawców
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Interfejs naruszeń w chmurze obliczeniowej, wyjście, środki umowne, podwykonawstwo i zapisy lokalizacji
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategia i nadzór nad relacjami dostawczymi
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planowanie, uzgadnianie, zarządzanie, monitorowanie i zakończenie relacji z dostawcą
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Ramy usuwania i dokumentacja
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Wdrożenie usuwania i wyjątki

1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące prywatności dla usług w chmurze obliczeniowej, w których organizacja działa jako podmiot przetwarzający PII lub podwykonawca przetwarzania, w tym usług SaaS, PaaS, IaaS, aplikacji hostowanych, zarządzanej chmury obliczeniowej, wsparcia chmurowego, przechowywania danych w chmurze obliczeniowej, analityki chmurowej oraz infrastruktury chmurowej, które przetwarzają PII w imieniu klientów.

1.2 Niniejsza polityka ma zastosowanie do przetwarzania w chmurze obliczeniowej realizowanego na podstawie umów z klientami, udokumentowanych poleceń klienta, poleceń nadrzędnego podmiotu przetwarzającego, uzgodnień z podwykonawcami przetwarzania, konfiguracji regionów chmury obliczeniowej, dostępu wsparcia chmurowego, administrowania usługą, kopii zapasowych, replikacji, rejestrowania, monitorowania, usuwania, zwrotu, wsparcia przy naruszeniach, wsparcia audytu oraz obowiązków wsparcia klienta.

1.3 Niniejsza polityka obejmuje:

1.3.1 zakres przetwarzania PII w chmurze obliczeniowej i zapisy poleceń;

1.3.2 dowody dotyczące umów z klientami i współdzielonej odpowiedzialności;

1.3.3 dowody izolacji tenantów, dostępu do chmury obliczeniowej, dostępu administracyjnego i rejestrowania;

1.3.4 nadzór nad podwykonawcami przetwarzania i łańcuchem dostaw chmury obliczeniowej;

1.3.5 lokalizację, dostęp zdalny i ścieżki międzynarodowego transferu;

1.3.6 dowody zwrotu, transferu, usunięcia, utylizacji i wyjścia;

1.3.7 wsparcie klienta w zakresie praw osób, których dane dotyczą, DPIA, audytów i reakcji na naruszenie;

1.3.8 dowody monitorowania, wyjątków, egzekwowania postanowień polityki i doskonalenia.

1.4 Niniejsza polityka nie tworzy odrębnego rejestru umów z klientami, rejestru usług chmurowych, rejestru izolacji tenantów, rejestru dostępu, rejestru logów, rejestru usuwania, rejestru wniosków o wsparcie, rejestru dowodów audytowych, rejestru naruszeń, rejestru podwykonawców przetwarzania ani komitetu zarządzania chmurą obliczeniową.

1.5 Niniejsza polityka nie zastępuje:

1.5.1 PII03 w zakresie inwentarza przetwarzania i własności podstawy prawnej;

1.5.2 PII06 w zakresie pełnego procesu obsługi praw osoby, której dane dotyczą;

1.5.3 PII07 w zakresie ryzyka dla prywatności i metodyki DPIA;

1.5.4 PII08 w zakresie bramek privacy by design i privacy by default;

1.5.5 PII09 w zakresie ogólnych środków kontroli gromadzenia, wykorzystywania, ujawniania i udostępniania;

1.5.6 PII10 w zakresie metodyki okresu przechowywania, usuwania i utylizacji;

1.5.7 PII12 w zakresie ogólnego nadzoru nad cyklem życia podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich;

1.5.8 PII13 w zakresie oceny mechanizmów międzynarodowego transferu;

1.5.9 PII14 w zakresie pełnej architektury bezpieczeństwa PII i kontroli dostępu;

1.5.10 PII15 w zakresie procesu zarządzania incydentami i naruszeniami;

1.5.11 PII17 w zakresie kontroli udokumentowanej informacji;

1.5.12 PII18 w zakresie monitorowania, audytu i doskonalenia PIMS.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby usługi podmiotu przetwarzającego i podwykonawcy przetwarzania PII w chmurze obliczeniowej były realizowane zgodnie z udokumentowanymi

poleceniami klienta, jasno określonym zakresem przetwarzania, kontrolowanymi uzgodnieniami z podwykonawcami przetwarzania, odpowiednimi obowiązkami w zakresie bezpieczeństwa chmury obliczeniowej, udokumentowaną lokalizacją i ścieżkami transferu, obowiązkami wsparcia klienta, wsparciem przy naruszeniach, zdolnością do usunięcia/zwrotu oraz dowodami umożliwiającymi wykazanie zgodności podczas audytu.

2.2 Niniejsza polityka wspiera gotowość do certyfikacji PIMS zgodnie z ISO/IEC 27701:2025 dla podmiotów przetwarzających w chmurze obliczeniowej i podwykonawców przetwarzania w chmurze obliczeniowej, pozostając jednocześnie zintegrowana z istniejącym zestawem polityk PIMS i kanonicznymi obiektami dowodowymi.

3. Cele

3.1 Cele niniejszej polityki są następujące:

3.1.1 Określenie zakresu przetwarzania PII w chmurze obliczeniowej przed onboardingiem klienta lub istotną zmianą.

3.1.2 Zapewnienie, że polecenia klienta są rejestrowane, przeglądane i wykonywane.

3.1.3 Utrzymywanie dowodów dotyczących podmiotu przetwarzającego i podwykonawcy przetwarzania w chmurze obliczeniowej w kanonicznych rejestrach PIMS.

3.1.4 Określenie dowodów współdzielonej odpowiedzialności, izolacji tenantów, dostępu, rejestrowania i lokalizacji bez powielania polityki bezpieczeństwa PII.

3.1.5 Kontrolowanie dowodów onboardingu, zmian, obowiązków przenoszonych na dalsze podmioty i monitorowania podwykonawców przetwarzania.

3.1.6 Wspieranie klientów w zakresie praw osób, których dane dotyczą, DPIA, wniosków audytowych i reakcji na naruszenie.

3.1.7 Zapewnienie zachowania dowodów zwrotu, usunięcia, transferu i utylizacji przy wyjściu.

3.1.8 Monitorowanie środków kontroli podmiotu przetwarzającego w chmurze obliczeniowej i inicjowanie działań korygujących z wykorzystaniem REG12.

4. Postanowienia polityki

4.1 Zakres przetwarzania w chmurze obliczeniowej i polecenia klienta

4.1.1 [Processor] Privacy Lead / PIMS Manager MUST zarejestrować każdą usługę przetwarzania PII w chmurze obliczeniowej, rolę klienta w przetwarzaniu, źródło polecenia klienta, kategorie PII, kategorie osób, których dane dotyczą, cel usługi, lokalizację przetwarzania, zależność od podwykonawcy przetwarzania, zależność dotyczącą usuwania oraz flagę transferu w REG02 i REG08 przed onboardingiem klienta lub istotną zmianą usługi.

4.1.2 [Processor] Process Owner / Business Owner MUST zarejestrować udokumentowane polecenia klienta dotyczące przetwarzania PII w chmurze obliczeniowej w REG08 przed rozpoczęciem przetwarzania.

4.1.3 [Subprocessor] Process Owner / Business Owner MUST zarejestrować polecenia nadrzędnego podmiotu przetwarzającego lub polecenia zatwierdzone przez klienta w REG08 przed przetwarzaniem PII jako podwykonawca przetwarzania w chmurze obliczeniowej.

4.1.4 [Processor] Privacy Lead / PIMS Manager MUST zarejestrować stosowalność zabezpieczeń podmiotu przetwarzającego w chmurze obliczeniowej w REG03 przed udostępnieniem lub istotną zmianą nowej usługi przetwarzania PII w chmurze obliczeniowej.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor MUST dokonać przeglądu każdego polecenia klienta, które wydaje się niespójne z udokumentowanymi obowiązkami klienta, wymaganiami PIMS lub zatwierdzonym zakresem usługi, w REG12, zanim organizacja podejmie działania na podstawie tego polecenia.

4.1.6 [Processor] Process Owner / Business Owner MUST zarejestrować każde proponowane przetwarzanie PII klienta poza udokumentowanymi poleceniami klienta w REG12 i uzyskać zatwierdzenie Privacy Lead / PIMS Manager przed rozpoczęciem przetwarzania.

4.2 Konfiguracja chmury obliczeniowej, izolacja tenantów, dostęp i rejestrowanie

4.2.1 [Processor] Information Security Lead MUST zarejestrować granicę współdzielonej odpowiedzialności w chmurze obliczeniowej dla dostępu do PII, administracji, rejestrowania, kopii zapasowych, szyfrowania, zarządzania podatnościami i usuwania w REG08 przed onboardingiem klienta lub istotną zmianą usługi.

4.2.2 [Processor] System Owner / Application Owner MUST zwalidować izolację tenantów lub środki segregacji klientów w REG12 przed użyciem produkcyjnym i po istotnej zmianie architektury.

4.2.3 [Processor] System Owner / Application Owner MUST przyznać administracyjny dostęp chmurowy do PII klienta wyłącznie po zarejestrowaniu w REG12 zatwierdzonej potrzeby biznesowej, zakresu dostępu, czasu trwania dostępu i częstotliwości przeglądu.

4.2.4 [Processor] Information Security Lead MUST dokonywać przeglądu uprzywilejowanego dostępu chmurowego, dostępu wsparcia, dostępu do PII klienta oraz pokrycia rejestrowaniem w REG12 co najmniej kwartalnie.

4.2.5 [Processor] System Owner / Application Owner MUST zwalidować rozdzielenie środowisk produkcyjnych, stagingowych, testowych i wsparcia dla PII klienta w REG12 przed wydaniem oraz po istotnej zmianie środowiska.

4.2.6 [Processor] System Owner / Application Owner MUST zarejestrować lokalizacje kopii zapasowych, replikacji, przechowywania logów i dostępu wsparcia dla PII klienta w chmurze obliczeniowej w REG02, REG08 lub REG09 przed włączeniem lub zmianą tych lokalizacji.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wyjątki

9.1 [Processor] Process Owner / Business Owner MUST wystąpić o wyjątek dotyczący podmiotu przetwarzającego w chmurze obliczeniowej w REG12 przed onboardingiem, wydaniem, odnowieniem lub dalszym korzystaniem, gdy wymagane dowody poleceń klienta, podwykonawców przetwarzania, lokalizacji, dostępu, rejestrowania, usuwania lub interfejsu incydentowego są niekompletne.

9.2 [Processor] Data Protection Officer / Privacy Advisor MUST dokonywać przeglądu istotnych z punktu widzenia prywatności wniosków o wyjątek dotyczący podmiotu przetwarzającego w chmurze obliczeniowej w REG12 przed zatwierdzeniem, gdy wyjątek wpływa na polecenia klienta, wsparcie osób, których dane dotyczą, transfery, podwykonawców przetwarzania, usuwanie, wsparcie przy naruszeniu lub PII o istotnym wpływie.

9.3 [Processor] Top Management MUST zatwierdzić wyjątki wysokiego ryzyka lub istotne wyjątki dotyczące podmiotu przetwarzającego w chmurze obliczeniowej w REG12 przed wejściem wyjątku w życie.

9.4 [Processor] Privacy Lead / PIMS Manager MUST przypisać datę wygaśnięcia, właściciela remediacji, datę przeglądu oraz informację o ryzyku rezydualnym w REG12 dla każdego zatwierdzonego wyjątku dotyczącego podmiotu przetwarzającego w chmurze obliczeniowej przed zatwierdzeniem.

10. Egzekwowanie postanowień polityki

10.1 [Processor] Privacy Lead / PIMS Manager MUST zablokować onboarding klienta, wydanie usługi, odnowienie lub dalsze przetwarzanie, gdy wymagane dowody w REG02, REG03, REG08, REG09, REG10 lub REG12 są brakujące przed rozpoczęciem lub kontynuacją przetwarzania.

10.2 [Processor] System Owner / Application Owner MUST wyłączyć niezatwierdzony dostęp chmurowy, niezatwierdzone użycie regionu, niezatwierdzoną replikację, niezatwierdzony dostęp wsparcia lub niezatwierdzony przepływ danych do podwykonawcy przetwarzania w ciągu jednego dnia roboczego od decyzji egzekwującej oraz zarejestrować zakończenie w REG08 lub REG12.

10.3 [Processor] Vendor / Procurement Owner MUST zawiesić nowe przetwarzanie PII przez niezatwierdzonego lub niezgodnego podwykonawcę przetwarzania w chmurze obliczeniowej do czasu kompletności dowodów działań korygujących w REG08.

10.4 [Processor] Incident Response Coordinator MUST eskalować niedotrzymane terminy powiadomienia klienta o incydencie w REG10 i REG12 w ciągu jednego dnia roboczego od identyfikacji.

10.5 [Processor] Internal Audit / Compliance Reviewer MUST zweryfikować skuteczność działań korygujących w przypadku dużych lub powtarzających się niezgodności dotyczących podmiotu przetwarzającego w chmurze obliczeniowej w REG12 w ciągu 60 dni od zamknięcia działań korygujących.

11. Przegląd i utrzymanie

11.1 [Processor] Privacy Lead / PIMS Manager MUST dokonywać przeglądu niniejszej polityki w REG12 corocznie oraz w ciągu 30 dni po istotnej zmianie obowiązków podmiotu przetwarzającego w chmurze obliczeniowej, architektury chmury obliczeniowej, nadzoru nad podwykonawcami przetwarzania, wsparcia klienta, zdolności do usuwania lub wymagań certyfikacyjnych.

11.2 [Processor] Vendor / Procurement Owner MUST dokonywać przeglądu zapisów dotyczących podwykonawców przetwarzania w chmurze obliczeniowej i zależności od usług chmurowych w REG08 co najmniej raz w roku oraz przed odnowieniem.

11.3 [Processor] System Owner / Application Owner MUST dokonywać przeglądu izolacji tenantów, dostępu uprzywilejowanego, rejestrowania, kopii zapasowych, replikacji i dowodów usuwania w REG12 co najmniej raz w roku oraz po istotnej zmianie architektury.

11.4 [Processor] Privacy Lead / PIMS Manager MUST dokonywać przeglądu zapisów dotyczących lokalizacji chmurowych i ścieżek transferu w REG09 co najmniej raz w roku oraz w ciągu 15 dni roboczych po istotnej zmianie lokalizacji, dostępu wsparcia, kopii zapasowych lub podwykonawcy przetwarzania.

11.5 [Processor] Privacy Lead / PIMS Manager MUST zaktualizować REG03 w ciągu 15 dni roboczych po zatwierdzonych zmianach polityki wpływających na stosowalność zabezpieczeń podmiotu przetwarzającego w chmurze obliczeniowej.

11.6 [All] Top Management MUST zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.

12. Powiązane polityki

12.1 Niniejszą politykę wspierają następujące powiązane polityki:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności

12.3 PII02 - Polityka ról, obowiązków i rozliczalności w zakresie prywatności

12.4 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej

12.5 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.6 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.7 PII08 - Polityka privacy by design i privacy by default

12.8 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII

12.9 PII10 - Polityka okresu przechowywania, usuwania i utylizacji PII

12.10 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich

12.11 PII13 - Polityka międzynarodowego transferu PII

12.12 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.13 PII15 - Polityka zarządzania incydentami i naruszeniami PII

12.14 PII17 - Polityka udokumentowanej informacji i zarządzania dowodami PIMS

12.15 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

12.16 PII20 - Polityka prywatności dzieci

12.17 PII21 - Polityka prywatności w zakresie AI i zautomatyzowanego podejmowania decyzji

12.18 PII22 - Polityka prywatności w marketingu i plików cookie

12.19 PII24 - Polityka CCTV i monitoringu fizycznego

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest mapowana do następujących norm i regulacji. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz wskazuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].