					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII15					Tytuł dokumentu: **Polityka zarządzania incydentami i naruszeniami ochrony PII**							
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	Stosowalność	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacja PIMS oraz udokumentowane dowody dotyczące naruszeń ochrony PII
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Powiązanie kontroli operacyjnej, oceny ryzyka dla prywatności i postępowania z ryzykiem
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, ocena, niezgodność, działanie korygujące i doskonalenie
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planowanie zarządzania incydentami i przygotowanie do przetwarzania PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reagowanie na incydenty bezpieczeństwa informacji obejmujące PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Wymagania prawne, ustawowe, regulacyjne i umowne oraz ochrona zapisów
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Umowa klienta z podmiotem przetwarzającym oraz wsparcie obowiązków klienta
GDPR	Article 5(2); Article 24	Controller	Supporting	Rozliczalność i odpowiedzialność administratora
GDPR	Article 26	Joint Controller	Supporting	Koordynacja odpowiedzialności współadministratorów za naruszenia

GDPR	Article 28	Both	Supporting	Pomoc podmiotu przetwarzającego i obowiązki umowne podmiotu przetwarzającego
GDPR	Article 32	Both	Supporting	Bezpieczeństwo przetwarzania oraz zdolność wykrywania naruszeń
GDPR	Article 33	Both	Primary	Zgłaszanie naruszeń ochrony danych osobowych oraz dokumentowanie naruszeń
GDPR	Article 34	Controller	Primary	Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
GDPR	Article 39	Conditional	Supporting	Doradztwo DPO, monitorowanie, współpraca i wsparcie punktu kontaktowego
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zasady bezpieczeństwa informacji i zgodności w zakresie prywatności
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odpowiedzialności dotyczące reagowania na incydenty PII oraz zgłaszanie zdarzeń
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planowanie incydentów, ocena, reagowanie, wyciągnięte wnioski oraz gromadzenie dowodów
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Cykl życia procesu zarządzania incydentami
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10;	Both	Supporting	Polityka incydentów, plan, świadomość,

	Clause 11; Clause 12			testowanie i wyciągnięte wnioski
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operacje wykrywania, powiadamiania, triage, analizy, reagowania i raportowania
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Oczekiwania dotyczące powiadamiania przez podmiot przetwarzający w chmurze obliczeniowej oraz zapisów naruszeń
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Raportowanie istotnych incydentów, jeżeli ma zastosowanie
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Zarządzanie incydentami ICT, klasyfikacja i raportowanie, jeżeli mają zastosowanie

1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące identyfikowania, zgłaszania, triage, oceny, powstrzymywania, powiadamiania, dokumentowania, zamykania oraz doskonalenia na podstawie incydentów PII i naruszeń ochrony PII w zakresie PIMS.

1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 organizacji działającej jako administrator PII;

1.2.2 organizacji działającej jako współadministrator, gdy wymagana jest koordynacja odpowiedzialności za naruszenie;

1.2.3 organizacji działającej jako podmiot przetwarzający PII;

1.2.4 organizacji działającej jako podwykonawca przetwarzania;

1.2.5 systemów, aplikacji, usług, procesów, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich, które przetwarzają, przechowują, przesyłają, wspierają, uzyskują dostęp do PII lub w inny sposób wpływają na PII w zakresie PIMS.

1.3 Niniejsza polityka wykorzystuje REG10 - Rejestr incydentów i naruszeń ochrony PII jako podstawowy obiekt dowodowy na potrzeby zarządzania incydentami PII i naruszeniami ochrony PII.

1.4 Niniejsza polityka wykorzystuje wspierające obiekty dowodowe w następujący sposób:

1.4.1 REG01 w odniesieniu do zakresu PIMS, właściwych zainteresowanych stron oraz kontekstu zgłoszeń prawnych, umownych, sektorowych i klienckich.

1.4.2 REG02 w odniesieniu do objętych zdarzeniem czynności przetwarzania, kategorii PII, kategorii osób, których dane dotyczą, celów i systemów.

1.4.3 REG03 w odniesieniu do Deklaracji stosowania oraz aktualizacji stosowalności środków kontrolnych.

1.4.4 REG04 w odniesieniu do powiązania z ryzykiem dla prywatności, DPIA i ryzykiem rezydualnym.

1.4.5 REG08 w odniesieniu do dowodów interfejsu incydentowego z podmiotami przetwarzającymi, podwykonawcami przetwarzania, klientami, dostawcami i stronami trzecimi.

1.4.6 REG09 w odniesieniu do powiązania z transferami międzynarodowymi, gdy incydent wpływa na przetwarzanie transgraniczne.

1.4.7 REG11 w odniesieniu do dowodów szkoleń, świadomości i kompetencji w zakresie reagowania na incydenty.

1.4.8 REG12 w odniesieniu do dowodów audytu, niezgodności, działań korygujących i doskonalenia.

1.5 Niniejsza polityka opiera się na powiązanych politykach PIMS w zakresie specjalistycznych środków kontrolnych:

1.5.1 PII03 reguluje inwentarz przetwarzania oraz zapisy podstaw prawnych.

1.5.2 PII04 reguluje klauzulę informacyjną i środki kontroli przejrzystości poza komunikacją dotyczącą konkretnych naruszeń.

1.5.3 PII06 reguluje wnioski o realizację praw osób, których dane dotyczą, powstające przed incydentem, w jego trakcie lub po nim.

1.5.4 PII07 reguluje metodykę oceny ryzyka dla prywatności i DPIA.

1.5.5 PII08 reguluje środki kontroli privacy by design i privacy by default.

1.5.6 PII10 reguluje środki kontroli retencji, usuwania i utylizacji.

1.5.7 PII12 reguluje środki kontroli relacji prywatności z podmiotami przetwarzającymi, podwykonawcami przetwarzania, dostawcami i stronami trzecimi.

1.5.8 PII13 reguluje mechanizmy międzynarodowego transferu PII oraz zapisy ryzyka transferu.

1.5.9 PII14 reguluje zapobiegawcze i detekcyjne środki bezpieczeństwa PII oraz kontroli dostępu.

1.5.10 PII16 reguluje szkolenia, świadomość i kompetencje w zakresie prywatności.

1.5.11 PII17 reguluje udokumentowane informacje i zarządzanie dowodami.

1.5.12 PII18 reguluje monitorowanie, audyt wewnętrzny, przegląd zarządzania, niezgodności, działania korygujące i ciągłe doskonalenie.

1.6 Na potrzeby niniejszej polityki:

1.6.1 „Incydent PII" oznacza podejrzewane lub potwierdzone zdarzenie, które wpłynęło, mogło wpłynąć lub mogłoby racjonalnie wpłynąć na poufność, integralność, dostępność, zgodne z prawem przetwarzanie lub uprawnione postępowanie z PII.

1.6.2 „Naruszenie ochrony PII" oznacza potwierdzony incydent PII obejmujący nieuprawnione, bezprawne, przypadkowe lub niezamierzone zniszczenie, utratę, zmianę, ujawnienie, dostęp, niedostępność lub kompromitację PII.

1.6.3 „Ocena naruszenia" oznacza udokumentowaną ocenę tego, czy incydent PII stanowi naruszenie ochrony PII, jakie PII i osoby, których dane dotyczą, są objęte zdarzeniem, jakie ryzyka mogą powstać, jakie zgłoszenia lub komunikaty są wymagane oraz jakie działania zaradcze są potrzebne.

1.6.4 „Świadomość" oznacza moment, w którym organizacja ma uzasadniony stopień pewności, że wystąpił incydent bezpieczeństwa lub prywatności oraz że PII zostały lub mogły zostać naruszone.

1.6.5 „Incydent PII o istotnym wpływie" oznacza incydent PII obejmujący przetwarzanie wysokiego ryzyka, szczególne kategorie PII lub bardzo wrażliwe PII, PII na dużą skalę, osoby wymagające szczególnej ochrony, klientów regulowanych, wpływ wielojurysdykcyjny, istotny wpływ na klienta, kompromitację dostępu uprzywilejowanego, ekspozycję publiczną, ransomware, niedostępność usług albo istotny wpływ operacyjny lub reputacyjny.

1.6.6 „Istotna zmiana dotycząca incydentu" oznacza nowe lub zmienione informacje wpływające na zakres incydentu, wagę, kategorie PII, wpływ na osoby, których dane dotyczą, decyzję o powiadomieniu, wpływ na klienta, przyczynę źródłową, powstrzymanie, odzyskiwanie, działanie korygujące lub obowiązki raportowania zewnętrznego.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby incydenty PII i naruszenia ochrony PII były obsługiwane spójnie, niezwłocznie, zgodnie z prawem, bezpiecznie oraz z dowodami umożliwiającymi wykazanie zgodności podczas audytu.

2.2 Niniejsza polityka wspiera rozliczalność poprzez wymaganie, aby incydenty PII i naruszenia ochrony PII były rejestrowane w REG10 oraz powiązane z objętymi zdarzeniem zapisami przetwarzania, ryzykami dla prywatności, relacjami z podmiotami przetwarzającymi i podwykonawcami przetwarzania, zapisami transferów, działaniami korygującymi oraz zapisami szkoleń, jeżeli zostaną wyzwolone.

2.3 Niniejsza polityka zapewnia obsługę obowiązków administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania według odrębnych reguł stosowalności, przy jednoczesnym utrzymaniu jednego zintegrowanego modelu dowodowego dla incydentów i naruszeń.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 zapewnienie niezwłocznego zgłaszania i rejestrowania podejrzewanych incydentów PII;

3.1.2 zapewnienie, aby incydenty PII podlegały triage i klasyfikacji z użyciem spójnych kryteriów;

3.1.3 zapewnienie, aby oceny naruszeń uwzględniały objęte zdarzeniem PII, osoby, których dane dotyczą, systemy, czynności przetwarzania, podmioty przetwarzające, podwykonawców przetwarzania, transfery, ryzyka i działania zaradcze;

3.1.4 zapewnienie dokumentowania decyzji dotyczących zgłoszenia przez administratora oraz komunikacji z osobami, których dane dotyczą;

3.1.5 zapewnienie, aby zgłoszenia naruszeń przez podmioty przetwarzające i podwykonawców przetwarzania do klientów lub podmiotów nadrzędnych były dokonywane bez zbędnej zwłoki i zgodnie z właściwymi umowami;

3.1.6 zapewnienie zachowania i ochrony dowodów podczas obsługi incydentu;

3.1.7 zapewnienie śledzenia powstrzymania, usunięcia zagrożenia, odzyskiwania i walidacji za pośrednictwem REG10;

3.1.8 zapewnienie oceny wyzwalaczy raportowania regulowanego, umownego, klienckiego i sektorowego, jeżeli mają zastosowanie;

3.1.9 zapewnienie, aby wyciągnięte wnioski z incydentów skutkowały działaniami korygującymi i ciągłym doskonaleniem;

3.1.10 zapewnienie dostępności zapisów incydentów i naruszeń na potrzeby audytu, przeglądu zarządzania, zapewnienia dla klientów i przeglądu regulacyjnego, jeżeli mają zastosowanie.

4. Postanowienia polityki

4.1 Gotowość do obsługi incydentów i przyjmowanie zgłoszeń

4.1.1 [Both] Privacy Lead / PIMS Manager MUSI utrzymywać w REG10 kryteria obsługi incydentów PII i naruszeń ochrony PII co najmniej raz w roku oraz po każdej istotnej zmianie zakresu PIMS, kontekstu prawnego, obowiązków umownych lub przetwarzania wysokiego ryzyka.

4.1.2 [All] Incident Response Coordinator MUSI zarejestrować każdy zgłoszony lub wykryty podejrzewany incydent PII w REG10 w ciągu jednego dnia roboczego od otrzymania, albo wcześniej, gdy może zostać wyzwolony właściwy termin powiadomienia lub raportowania do klienta.

4.1.3 [Both] System Owner / Application Owner MUSI zachować właściwe logi systemowe, alerty, zapisy dostępu, dowody konfiguracji i dowody odzyskiwania powiązane z REG10, gdy podejrzewany incydent wpływa na system lub aplikację przetwarzającą PII.

4.1.4 [Both] Information Security Lead MUSI zakończyć wstępny techniczny triage każdego zdarzenia bezpieczeństwa obejmującego PII w ciągu 24 godzin od wykrycia oraz zarejestrować w REG10 wstępną wagę, objęte zdarzeniem aktywa i status powstrzymania.

4.2 Klasyfikacja i ocena naruszenia

4.2.1 [Both] Incident Response Coordinator MUSI sklasyfikować każdy wpis REG10 jako zdarzenie niedotyczące PII, podejrzewany incydent PII, potwierdzony incydent PII albo potwierdzone naruszenie ochrony PII w ciągu 24 godzin od przyjęcia lub zaktualizować zapis REG10 o powód, dla którego klasyfikacja pozostaje oczekująca.

4.2.2 [Both] Privacy Lead / PIMS Manager MUSI zidentyfikować objętą zdarzeniem czynność przetwarzania, kategorie PII, kategorie osób, których dane dotyczą, systemy, podmioty przetwarzające, podwykonawców przetwarzania, lokalizacje transferów i ryzyka dla prywatności w REG02, REG04, REG08, REG09 i REG10 przed sfinalizowaniem decyzji o zgłoszeniu naruszenia.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUSI ocenić ryzyko dla objętych zdarzeniem osób, których dane dotyczą, dla każdego potwierdzonego lub zasadnie

podejrzewanego naruszenia ochrony PII oraz zarejestrować w REG10 rekomendację dotyczącą powiadomienia, uzasadnienie ryzyka i poradę przed podjęciem decyzji o zgłoszeniu zewnętrznym.

4.2.4 [Processor] Privacy Lead / PIMS Manager MUSI zidentyfikować objętego zdarzeniem administratora lub klienta oraz właściwe umowne wymagania dotyczące powiadomienia niezwłocznie po uzyskaniu przez organizację świadomości naruszenia ochrony PII wpływającego na PII klienta, a także MUSI zarejestrować wynik w REG08 i REG10.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager MUSI zweryfikować uzgodnioną odpowiedzialność za naruszenie, wiodącą odpowiedzialność komunikacyjną i ustalenia koordynacyjne przed każdym zewnętrznym zgłoszeniem lub komunikatem współadministratora oraz MUSI zarejestrować decyzję w REG08 i REG10.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUSI ocenić właściwe wyzwalacze raportowania prawnego, sektorowego, dla sektora finansowego, cyberbezpieczeństwa, umownego, klienckiego i do odbiorców usług dla każdego incydentu PII o istotnym wpływie oraz zarejestrować wynik stosowalności w REG01, REG08 i REG10.

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

9. Wyjątki

9.1.1 [Both] Privacy Lead / PIMS Manager MUSI zarejestrować każdy wyjątek od niniejszej polityki w REG12 przed wdrożeniem albo w ciągu 24 godzin po działaniu awaryjnym, jeżeli wcześniejsze zatwierdzenie nie było wykonalne.

9.1.2 [Both] Top Management MUSI zatwierdzić każdy wyjątek, który istotnie wpływa na termin zgłoszenia naruszenia, komunikację publiczną, zobowiązanie wobec klienta, zachowanie dowodów lub ryzyko dla osoby, której dane dotyczą, przed zamknięciem incydentu, z zachowaniem dowodów zatwierdzenia w REG10 i REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUSI udokumentować poradę dla każdego opóźnionego zgłoszenia, decyzji o braku zgłoszenia lub wyjątkowego podejścia komunikacyjnego przed zamknięciem incydentu, z zachowaniem porady w REG10.

9.1.4 [Both] Vendor / Procurement Owner MUSI zarejestrować wyjątki wynikające z działań dostawcy, podmiotu przetwarzającego, podwykonawcy przetwarzania lub klienta, które wpływają na reagowanie na incydenty, w REG08 i REG12 w ciągu pięciu dni roboczych od zidentyfikowania wyjątku.

10. Egzekwowanie

10.1.1 [All] Process Owner / Business Owner MUSI eskalować brak zgłoszenia podejrzewanego incydentu PII, zachowania dowodów, wykonania przypisanych działań lub współpracy przy ocenie naruszenia do Privacy Lead / PIMS Manager w ciągu dwóch dni roboczych od wykrycia, z zachowaniem dowodów w REG12.

10.1.2 [Both] Privacy Lead / PIMS Manager MUSI zarejestrować niezgodność REG12, gdy naruszenie niniejszej polityki wpływa na przyjmowanie incydentów, triage, powstrzymanie, powiadomienie, integralność dowodów, komunikację lub działanie korygujące.

10.1.3 [Both] Vendor / Procurement Owner MUSI zainicjować remediację dostawcy lub podmiotu przetwarzającego za pośrednictwem REG08 i REG12 w ciągu pięciu dni roboczych, gdy podmiot przetwarzający, podwykonawca przetwarzania, dostawca lub inna strona trzecia nie spełnia uzgodnionych obowiązków dotyczących incydentu lub naruszenia.

10.1.4 [Both] Top Management MUSI dokonać przeglądu istotnych lub powtarzających się niezgodności w zarządzaniu incydentami podczas najbliższego zaplanowanego przeglądu zarządzania, z zachowaniem decyzji i wymaganych działań w REG12.

11. Przegląd i utrzymanie

11.1.1 [Both] Privacy Lead / PIMS Manager MUSI dokonywać przeglądu niniejszej polityki co najmniej raz w roku oraz rejestrować wynik przeglądu, wymagane zmiany i status zatwierdzenia w REG12.

11.1.2 [Both] Incident Response Coordinator MUSI wyzwolić przegląd poincydentalny niniejszej polityki w ciągu 30 dni kalendarzowych po zamknięciu każdego incydentu PII o istotnym wpływie lub potwierdzonego naruszenia ochrony PII, z zachowaniem dowodów przeglądu w REG10 i REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager MUSI dokonać przeglądu niniejszej polityki w ciągu 30 dni kalendarzowych od uzyskania świadomości istotnej zmiany właściwych wymagań prawnych, sektorowych, klienckich, umownych, dotyczących podmiotów przetwarzających, podwykonawców przetwarzania lub transferów związanych z raportowaniem incydentów, z zachowaniem dowodów przeglądu w REG01, REG08, REG09 i REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer MUSI dokonywać przeglądu wdrożenia niniejszej polityki co najmniej raz w roku w ramach programu audytu wewnętrznego PIMS, z zachowaniem ustaleń z audytu i działań korygujących w REG12.

11.1.5 [Both] Top Management MUSI dokonywać przeglądu trendów incydentów, istotnych naruszeń, skuteczności powiadamiania, przeterminowanych działań korygujących i skuteczności polityki podczas zaplanowanego przeglądu zarządzania, z zachowaniem wyników w REG12.

12. Powiązane polityki

12.1 Niniejszą politykę należy czytać łącznie z:

12.1.1 PII01 - Polityka systemu zarządzania informacjami o prywatności

12.1.2 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności

12.1.3 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.1.4 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.1.5 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.1.6 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.1.7 PII08 - Polityka privacy by design i privacy by default

12.1.8 PII10 - Polityka retencji, usuwania i utylizacji PII

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

12.1.10 PII13 - Polityka międzynarodowego transferu PII

12.1.11 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.1.12 PII16 - Polityka szkoleń, świadomości i kompetencji w zakresie prywatności

12.1.13 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.1.14 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].