					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII01					Tytuł dokumentu: **Polityka systemu zarządzania informacjami o prywatności**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontekst i określenie roli PIMS
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Zainteresowane strony i wymagania
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	Zakres PIMS
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Ustanowienie i doskonalenie PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Przywództwo i zaangażowanie
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Polityka prywatności
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Role i uprawnienia
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Ryzyka i szanse
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Ocena ryzyka dla prywatności
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Postępowanie z ryzykiem dla prywatności i SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Cele dotyczące prywatności
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Planowane zmiany PIMS
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Zasoby
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetencje
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Świadomość
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Komunikacja
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Udokumentowane informacje
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Planowanie i nadzór operacyjny

ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operacyjna ocena ryzyka dla prywatności
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operacyjne postępowanie z ryzykiem dla prywatności
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorowanie i ocena
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audyt wewnętrzny
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Przegląd zarządzania
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Ciągłe doskonalenie
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Niezgodność i działanie korygujące
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Zapisy ładu zarządczego po stronie administratora
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Umowa i cele po stronie podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Powiązanie polityki bezpieczeństwa PII
GDPR	Article 5(2)	Controller	Supporting	Dowody rozliczalności
GDPR	Article 24	Controller	Supporting	Środki i polityka administratora
GDPR	Article 26	Joint Controller	Supporting	Uzgodnienia współadministratorów
GDPR	Article 28	Both	Supporting	Ład zarządczy dotyczący podmiotów przetwarzających
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania
GDPR	Article 32	Both	Supporting	Bezpieczeństwo przetwarzania
GDPR	Article 35	Controller	Supporting	Ład zarządczy DPIA
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Środki kontrolne i zasady prywatności

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Proces PIA i przygotowanie
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	Program ochrony PII i polityka
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integracja organizacyjnego ryzyka dla prywatności

1. Zakres

1.1 Niniejsza polityka ustanawia system zarządzania informacjami o prywatności organizacji dla przetwarzania PII w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania.

1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 zakresu PIMS, kontekstu, zainteresowanych stron i granic organizacyjnych;

1.2.2 określania roli PIMS dla czynności przetwarzania PII;

1.2.3 polityki prywatności, celów dotyczących prywatności, oceny ryzyka dla prywatności, postępowania z ryzykiem dla prywatności oraz Deklaracji stosowania PIMS;

1.2.4 ładu zarządczego PIMS, monitorowania, audytu wewnętrznego, przeglądu zarządzania, niezgodności, działań korygujących i ciągłego doskonalenia;

1.2.5 udokumentowanych informacji i dowodów potrzebnych do wykazania zgodności PIMS i rozliczalności.

1.3 Na potrzeby niniejszej polityki istotna zmiana oznacza każdą zmianę, która wpływa na zakres PIMS, cele przetwarzania PII, kategorie PII, kategorie osób, których dane dotyczą, lokalizacje przetwarzania, przydział roli administratora lub podmiotu przetwarzającego, architekturę systemu, uzgodnienia z dostawcami lub podwykonawcami przetwarzania, profil ryzyka dla prywatności, mające zastosowanie obowiązki prawne lub umowne albo zakres certyfikacji.

2. Cel

2.1 Niniejsza polityka określa obowiązkowe wymagania ładu zarządczego dotyczące ustanawiania, wdrażania, utrzymywania, monitorowania i ciągłego doskonalenia PIMS.

2.2 Celem niniejszej polityki jest zapewnienie, aby organizacja mogła wykazać rozliczalne, oparte na ryzyku i dowodach zarządzanie przetwarzaniem PII we wszystkich mających zastosowanie rolach PIMS.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 określenie zakresu, kontekstu, granic i zastosowania ról PIMS;

3.1.2 przypisanie rozliczalności w ramach ładu zarządczego za PIMS z wykorzystaniem kanonicznych ról PIMS;

3.1.3 ustanowienie celów dotyczących prywatności oraz mierzalnych oczekiwań dotyczących wyników PIMS;

3.1.4 utrzymywanie Deklaracji stosowania PIMS dla wybranych i wyłączonych środków kontrolnych;

3.1.5 włączenie oceny ryzyka dla prywatności, postępowania z ryzykiem dla prywatności oraz ładu zarządczego DPIA do działania PIMS;

3.1.6 zapewnienie, aby obowiązki administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania były identyfikowane przed rozpoczęciem przetwarzania;

3.1.7 utrzymywanie dowodów gotowych do audytu na potrzeby gotowości do certyfikacji i ciągłego doskonalenia;

3.1.8 unikanie zbędnych ról, rejestrów, formularzy i powielonych operacyjnych środków kontrolnych.

4. Postanowienia polityki

4.1 Ustanowienie, kontekst i zakres PIMS

4.1.1 [Both] Top Management MUSI zatwierdzić zakres PIMS w REG01 przed początkowym wdrożeniem PIMS oraz w ciągu 30 dni od każdej istotnej zmiany.

4.1.2 [Both] Privacy Lead / PIMS Manager MUSI dokumentować zewnętrzne i wewnętrzne kwestie kontekstu prywatności w REG01 co roku oraz w ciągu 30 dni od każdej istotnej zmiany.

4.1.3 [Both] Privacy Lead / PIMS Manager MUSI dokumentować właściwe zainteresowane strony oraz ich wymagania dotyczące PIMS w REG01 co roku oraz w ciągu 30 dni od każdej istotnej zmiany.

4.1.4 [Both] Privacy Lead / PIMS Manager MUSI utrzymywać podsumowanie interakcji procesów PIMS w REG01 przed każdym przeglądem zarządzania.

4.2 Określanie roli PIMS

4.2.1 [Both] Process Owner / Business Owner MUSI sklasyfikować rolę PIMS organizacji dla każdej czynności przetwarzania PII w REG02 przed rozpoczęciem tej czynności przetwarzania.

4.2.2 [Joint Controller] Vendor / Procurement Owner MUSI udokumentować przydział odpowiedzialności współadministratorów w REG08 przed rozpoczęciem wspólnego przetwarzania.

4.2.3 [Processor] Vendor / Procurement Owner MUSI udokumentować instrukcje klienta dotyczące przetwarzania dla czynności wykonywanych jako podmiot przetwarzający w REG08 przed onboardingiem usługi.

4.2.4 [Subprocessor] Vendor / Procurement Owner MUSI udokumentować instrukcje klienta wyższego szczebla oraz zatwierdzone uzgodnienia dotyczące dalszego powierzenia przetwarzania w REG08 przed rozpoczęciem dalszego powierzenia przetwarzania.

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

9. Wyjątki

9.1 Wniosek o wyjątek i zatwierdzenie

9.1.1 [All] Process Owner / Business Owner MUSI udokumentować każdy wnioskowany wyjątek od niniejszej polityki w REG12 przed wystąpieniem odstępstwa.

9.1.2 [Both] Privacy Lead / PIMS Manager MUSI ocenić ryzyko dla prywatności związane z każdym wnioskowanym wyjątkiem w REG04 przed zatwierdzeniem.

9.1.3 [Both] Top Management MUSI zatwierdzać wyjątki, które przekraczają zaakceptowane progi ryzyka dla prywatności, w REG12 przed wdrożeniem.

9.1.4 [Both] Privacy Lead / PIMS Manager MUSI przeglądać aktywne wyjątki PIMS w REG12 kwartalnie aż do ich zamknięcia.

9.2 Zamknięcie wyjątku

9.2.1 [All] Process Owner / Business Owner MUSI udokumentować dowody zamknięcia wyjątku w REG12 do zatwierdzonej daty wygaśnięcia wyjątku.

9.2.2 [Both] Internal Audit / Compliance Reviewer MUSI zweryfikować dowody zamknięcia wygasłego wyjątku w REG12 podczas następnego planowanego audytu wewnętrznego.

10. Egzekwowanie postanowień polityki

10.1 Postępowanie z niezgodnościami

10.1.1 [All] Privacy Lead / PIMS Manager MUSI rejestrować podejrzewane niezgodności z niniejszą polityką w REG12 w ciągu pięciu dni roboczych od ich zidentyfikowania.

10.1.2 [All] Process Owner / Business Owner MUSI wdrożyć zatwierdzone działania korygujące w REG12 do przypisanego terminu po zatwierdzeniu niezgodności.

10.1.3 [All] Top Management MUSI przeglądać nierozwiązane istotne niezgodności PIMS w REG12 podczas każdego przeglądu zarządzania.

10.1.4 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących w REG12 w ciągu 30 dni od zgłoszonego zamknięcia.

10.2 Eskalacja

10.2.1 [All] Privacy Lead / PIMS Manager MUSI eskalować zaległe istotne działania korygujące do Top Management w REG12 w ciągu pięciu dni roboczych po terminie realizacji.

10.2.2 [All] Top Management MUSI rejestrować decyzje dotyczące zaległych istotnych działań korygujących w REG12 w ciągu 15 dni roboczych od eskalacji.

11. Przegląd i utrzymanie

11.1 Przegląd polityki

11.1.1 [All] Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 co roku oraz w ciągu 30 dni od każdej istotnej zmiany dotyczącej prawa, organizacji, przetwarzania, technologii lub zakresu certyfikacji.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUSI przekazać udokumentowaną poradę w REG12 przed zatwierdzeniem polityki, gdy zmieniają się istotne obowiązki dotyczące prywatności.

11.1.3 [All] Top Management MUSI zatwierdzać istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.4 [All] Privacy Lead / PIMS Manager MUSI zaktualizować REG01 i REG03 w ciągu 15 dni roboczych po zatwierdzeniu zmian polityki, które zmieniają zakres PIMS lub stosowanie środków kontrolnych.

11.1.5 [All] Privacy Lead / PIMS Manager MUSI zarejestrować komunikację zatwierdzonych zmian polityki w REG11 w ciągu 30 dni od publikacji.

12. Powiązane polityki

12.1 Niniejszą politykę wspierają następujące powiązane polityki:

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

12.3 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.4 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.5 PII08 - Polityka privacy by design i privacy by default

12.6 PII12 - Polityka dotycząca podmiotów przetwarzających, podwykonawców przetwarzania i udostępniania danych

12.7 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.8 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII

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

12.10 PII17 - Polityka zarządzania udokumentowanymi informacjami i dowodami PIMS

12.11 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana na następujące normy i regulacje. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz wskazuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Zmapowano na określanie kontekstu organizacyjnego, kwestii kontekstu prywatności oraz zastosowania roli administratora lub podmiotu przetwarzającego do czynności PIMS. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Zmapowano na identyfikowanie zainteresowanych stron, osób, których dane dotyczą, klientów, organów nadzorczych, podmiotów przetwarzających, podwykonawców przetwarzania oraz ich właściwych wymagań PIMS. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Zmapowano na definiowanie, zatwierdzanie, utrzymywanie i zmienianie udokumentowanego zakresu PIMS. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Zmapowano na ustanawianie, wdrażanie, utrzymywanie i doskonalenie procesów PIMS oraz ich interakcji. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Zmapowano na zatwierdzenie przez Top Management, zasoby, przegląd ładu zarządczego oraz przywództwo w zakresie skuteczności i doskonalenia PIMS. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Zmapowano na utrzymywanie niniejszej polityki prywatności jako zatwierdzonych udokumentowanych informacji oraz komunikowanie zmian polityki. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Zmapowano na przypisywanie i komunikowanie ról, odpowiedzialności i uprawnień PIMS. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Zmapowano na planowanie działań dotyczących ryzyk i szans PIMS z wykorzystaniem kontekstu, wymagań zainteresowanych stron, celów i danych wejściowych do doskonalenia. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Zmapowano na wymaganie przeprowadzania oceny ryzyka dla prywatności przed nowym lub istotnie zmienionym przetwarzaniem oraz utrzymywanie dowodów ryzyka dla prywatności. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Zmapowano na postępowanie z ryzykiem dla prywatności, dobór środków kontrolnych, powiązanie z programem bezpieczeństwa informacji oraz utrzymanie Deklaracji stosowania. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Zmapowano na ustanawianie, mierzenie, monitorowanie, komunikowanie i aktualizowanie celów PIMS. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Zmapowano na planowane zmiany PIMS oraz nadzór nad zmianami wpływającymi na zakres, role, środki kontrolne i udokumentowane informacje. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Zmapowano na określanie i zapewnianie zasobów potrzebnych do ustanowienia, działania, utrzymania i doskonalenia PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Zmapowano na oczekiwania dotyczące kompetencji oraz dowody wspierające odpowiedzialności PIMS i wykonywanie ról. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Zmapowano na świadomość polityki prywatności, wkład w skuteczność PIMS oraz konsekwencje niezgodności. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Zmapowano na komunikację wewnętrzną i zewnętrzną istotną dla ładu zarządczego PIMS, zmian polityki i eskalacji. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Zmapowano na tworzenie, utrzymywanie, kontrolę, gotowość dowodową i przechowywanie udokumentowanych informacji. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Zmapowano na planowanie, wdrażanie i nadzorowanie procesów operacyjnych PIMS oraz procesów dostarczanych zewnętrznie. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Zmapowano na wykonywanie ocen ryzyka dla prywatności w zaplanowanych odstępach czasu oraz gdy proponowane są lub występują znaczące zmiany. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Zmapowano na wdrażanie planów postępowania z ryzykiem dla prywatności oraz przechowywanie dowodów wyników postępowania z ryzykiem. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Zmapowano na monitorowanie, pomiar, analizę, ocenę, metryki i raportowanie skuteczności PIMS. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Zmapowano na planowanie audytu wewnętrznego, próbkowanie dowodów, wyniki audytu i niezależny przegląd. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Zmapowano na dane wejściowe do przeglądu zarządzania, przegląd wyników, wyniki przeglądu zarządzania i decyzje doskonalące. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Zmapowano na ciągłe doskonalenie poprzez przegląd zarządzania, metryki, śledzenie działań korygujących i utrzymanie polityki. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Zmapowano na postępowanie z niezgodnościami, działania korygujące, eskalację, zamknięcie i weryfikację skuteczności. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Zmapowano na zapisy celów przetwarzania po stronie administratora, powiązanie z podstawą prawną, określanie potrzeby DPIA, przydział odpowiedzialności współadministratorów oraz zapisy dowodowe przetwarzania. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Zmapowano na umowy klientów z podmiotem przetwarzającym, udokumentowane instrukcje klienta oraz ograniczenia celów po stronie podmiotu przetwarzającego. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Zmapowano na powiązanie polityki bezpieczeństwa PII, własność bazowego zestawu środków kontroli bezpieczeństwa PII oraz status środków kontroli bezpieczeństwa informacji w Deklaracji stosowania PIMS. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Zmapowano na dowody rozliczalności, zatwierdzenie polityki, klasyfikację roli przetwarzania, stosowanie środków kontrolnych, monitorowanie, audyt i zapisy działań korygujących. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Zmapowano na środki ładu zarządczego administratora, zatwierdzenie polityki, cele PIMS, przegląd skuteczności oraz udokumentowane dowody rozliczalności administratora. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Zmapowano na określanie i dokumentowanie przydziału odpowiedzialności współadministratorów przed rozpoczęciem wspólnego przetwarzania. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Zmapowano na zapisy ładu zarządczego dotyczące podmiotów przetwarzających i podwykonawców przetwarzania, instrukcje klienta dotyczące przetwarzania

oraz nadzór nad procesami dostarczanymi zewnętrznie. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Zmapowano na zapisy czynności przetwarzania, klasyfikację roli, zapisy rozliczalności przetwarzania oraz dowody przechowywane na potrzeby audytowalności. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Zmapowano na ład zarządczy dotyczący bazowego poziomu bezpieczeństwa PII, własność środków kontroli bezpieczeństwa, status wdrożenia zabezpieczeń oraz potwierdzenie nadzoru operacyjnego. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Zmapowano na określanie potrzeby DPIA oraz ocenę ryzyka dla prywatności przed kontynuowaniem przetwarzania przez administratora, które jest wysokiego ryzyka lub zostało istotnie zmienione. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Zmapowano na identyfikację środków kontroli prywatności, zasady prywatności, bezpieczeństwo informacji, zgodność w zakresie prywatności, audyt, dowody oraz oparty na ryzyku ład zarządczy prywatności. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Zmapowano na ład zarządczy PIA, określanie wyzwalaczy DPIA, przygotowanie PIA, kryteria ryzyka dla prywatności oraz udokumentowane dowody oceny ryzyka dla prywatności. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Zmapowano na wymagania programu ochrony PII, identyfikację wymagań ochrony PII, oparty na ryzyku prywatności dobór środków kontrolnych oraz kierunek polityki ochrony PII. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Zmapowano na zasady organizacyjnego ryzyka dla prywatności, zaangażowanie kierownictwa, integrację ryzyka dla prywatności z ładem zarządczym PIMS oraz zrozumienie roli organizacji w przetwarzaniu PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].