					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII16					Tytuł dokumentu: **Polityka szkoleń, świadomości i kompetencji w zakresie 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

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Zastosowanie	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Kompetencje i świadomość
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Komunikacja i udokumentowane dowody
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Kontrola operacyjna, pomiar i doskonalenie
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Świadomość, edukacja i szkolenia dotyczące przetwarzania PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Rozliczalność, nadzór nad podmiotami przetwarzającymi, bezpieczeństwo i zadania DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetencje, świadomość i szkolenia
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Wytyczne dotyczące świadomości, edukacji i szkoleń
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Bezpieczeństwo informacji i zgodność w zakresie prywatności

1. Zakres

1.1 Niniejsza polityka określa wymagania organizacji dotyczące szkoleń, świadomości i kompetencji w zakresie prywatności w ramach systemu zarządzania informacjami o prywatności.

1.2 Niniejsza polityka ma zastosowanie do personelu, wykonawców, personelu tymczasowego, właściwych stron trzecich, podmiotów przetwarzających, podwykonawców przetwarzania oraz innych zainteresowanych stron, których praca może wpływać na przetwarzanie PII, wyniki PIMS, prawa osób, których dane dotyczą, ryzyko dla prywatności, bezpieczeństwo informacji związane z PII, polecenia podmiotu przetwarzającego, incydenty dotyczące prywatności, udokumentowane informacje lub dowody zgodności.

1.3 Niniejsza polityka ma zastosowanie w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania.

1.4 Niniejsza polityka obejmuje:

1.4.1 identyfikację odbiorców szkoleń w zakresie prywatności;

1.4.2 szkolenie wdrożeniowe;

1.4.3 coroczne szkolenie przypominające;

1.4.4 szkolenia oparte na rolach i szkolenia wywołane zdarzeniem;

1.4.5 dowody ukończenia szkoleń;

1.4.6 eskalację nieukończenia szkolenia;

1.4.7 przegląd skuteczności szkoleń;

1.4.8 dowody potwierdzające realizację szkoleń podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich.

1.5 Niniejsza polityka nie tworzy odrębnej macierzy szkoleń, pulpitu szkoleń, rejestru zasobów ludzkich, rejestru kompetencji, rejestru dyscyplinarnego ani rejestru szkoleń klientów. Przypisania szkoleń, ukończenia, przypomnienia, dowody kompetencji i dowody świadomości są rejestrowane w REG11, natomiast wyjątki, eskalacje, niezgodności, działania korygujące i dowody przeglądu są rejestrowane w REG12. Dowody potwierdzające realizację szkoleń podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich są rejestrowane w REG08, jeżeli ma to zastosowanie.

1.6 Niniejsza polityka nie powiela:

1.6.1 przypisania rozliczalności ról w PII02;

1.6.2 wymagań dotyczących inwentarza przetwarzania i podstawy prawnej w PII03;

1.6.3 metodyki ryzyka dla prywatności i DPIA w PII07;

1.6.4 bramek privacy by design w PII08;

1.6.5 nadzoru nad cyklem życia podmiotu przetwarzającego w PII12;

1.6.6 działania zabezpieczeń PII i kontroli dostępu w PII14;

1.6.7 procesu obsługi incydentów i naruszeń PII w PII15;

1.6.8 nadzoru nad udokumentowanymi informacjami w PII17;

1.6.9 monitorowania, audytu wewnętrznego i nadzoru nad doskonaleniem w PII18.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby osoby, których praca wpływa na przetwarzanie PII, rozumiały swoje odpowiedzialności w zakresie prywatności, realizowały odpowiednie szkolenia w określonym cyklu, utrzymywały kompetencje właściwe dla roli oraz generowały audytowalne dowody szkoleń, świadomości i eskalacji.

2.2 Niniejsza polityka wspiera spójne wdrożenie PIMS przez wykorzystanie REG11 jako podstawowego obiektu dowodowego dla szkoleń i świadomości oraz REG08, REG10 i REG12 jako wspierających obiektów dowodowych.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 zdefiniowanie odbiorców szkoleń w zakresie prywatności;

3.1.2 zdefiniowanie wymagań dotyczących szkoleń wdrożeniowych;

3.1.3 zdefiniowanie wymagań dotyczących corocznych szkoleń przypominających;

3.1.4 zdefiniowanie wymagań dotyczących szkoleń z zakresu prywatności opartych na rolach;

3.1.5 rejestrowanie dowodów ukończenia w REG11;

3.1.6 eskalowanie nieukończenia szkolenia za pośrednictwem REG12;

3.1.7 utrzymywanie w REG08 dowodów potwierdzających realizację szkoleń podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich, jeżeli ma to zastosowanie;

3.1.8 dokonywanie przeglądu skuteczności szkoleń bez tworzenia nadmiernych metryk ani duplikowania rejestrów;

3.1.9 zapewnienie, aby treść szkoleń pozostawała zgodna z aktualnymi politykami PIMS i istotnymi obowiązkami w zakresie prywatności.

4. Postanowienia polityki

4.1 Odbiorcy szkoleń i przypisanie szkoleń

4.1.1 [All] Privacy Lead / PIMS Manager musi zdefiniować w REG11 kategorie odbiorców szkoleń PIMS przed rozpoczęciem każdego rocznego cyklu szkoleniowego.

4.1.2 [All] Process Owner / Business Owner musi zidentyfikować w REG11 personel, którego obowiązki obejmują przetwarzanie PII, przed wdrożeniem, przypisaniem roli lub istotną zmianą obowiązków.

4.1.3 [Conditional] System Owner / Application Owner musi zidentyfikować w REG11 użytkowników wymagających szkolenia z zakresu prywatności dotyczącego systemu PII, dostępu uprzywilejowanego lub administracji, zanim dostęp zostanie włączony lub istotnie zmieniony.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager musi zarejestrować w REG11 lub REG08 podział odpowiedzialności za szkolenia współadministratorów przed rozpoczęciem lub istotną zmianą wspólnej czynności przetwarzania.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor musi zidentyfikować w REG11 potrzeby rozszerzonego szkolenia w zakresie prywatności, zanim szkolenie zostanie przypisane do ról obsługujących przetwarzanie wysokiego ryzyka, szczególne kategorie PII, prawa osób, których dane dotyczą, DPIA, transfery międzynarodowe lub ocenę naruszeń.

4.1.6 [All] Privacy Lead / PIMS Manager musi zarejestrować w REG11 przypisanych odbiorców szkolenia, rodzaj szkolenia, wymagany termin ukończenia i właściciela dowodów przed rozpoczęciem każdego rocznego cyklu szkoleniowego.

4.2 Cykl szkoleń wdrożeniowych i corocznych

4.2.1 [All] Privacy Lead / PIMS Manager musi przypisać w REG11 bazowe szkolenie z zakresu świadomości prywatności w ciągu 10 dni roboczych od wdrożenia personelu mającego dostęp do PII lub odpowiedzialności w PIMS.

4.2.2 [All] Process Owner / Business Owner musi zapewnić, aby przypisany personel ukończył w REG11 szkolenie wdrożeniowe z zakresu prywatności przed zatwierdzeniem

nienadzorowanego dostępu do PII albo w ciągu 30 dni od wdrożenia, w zależności od tego, co nastąpi wcześniej.

4.2.3 [All] Privacy Lead / PIMS Manager musi przypisać w REG11 coroczne szkolenie przypominające z zakresu prywatności co najmniej raz na 12 miesięcy.

4.2.4 [All] Process Owner / Business Owner musi potwierdzić w REG11 status ukończenia corocznego szkolenia przypominającego przez przypisany personel do opublikowanego rocznego terminu.

4.2.5 [Conditional] Privacy Lead / PIMS Manager musi przypisać w REG11 ukierunkowane szkolenie przypominające w ciągu 30 dni po istotnej zmianie polityki prywatności, istotnej zmianie procesu PIMS, ustaleniu z audytu, powtarzającym się niezaliczeniu szkolenia lub właściwym wniosku wynikającym z incydentu PII.

[... 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 [All] Process Owner / Business Owner musi zarejestrować w REG12 wniosek o wyjątek dotyczący szkolenia z zakresu prywatności przed przedłużeniem wymaganego terminu ukończenia.

9.1.2 [All] Privacy Lead / PIMS Manager musi zatwierdzić albo odrzucić w REG12 wnioski o wyjątki dotyczące szkoleń z zakresu prywatności, zanim wyjątek stanie się aktywny.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musi doradzić w REG12 w sprawie wyjątków szkoleniowych przed zatwierdzeniem, jeżeli wyjątek wpływa na przetwarzanie wysokiego ryzyka, szczególne kategorie PII, obsługę praw, obsługę incydentów, transfery międzynarodowe lub dowody certyfikacyjne.

9.1.4 [Conditional] Top Management musi zatwierdzić w REG12 wyjątki dotyczące szkoleń z zakresu prywatności przed aktywacją, gdy wyjątek wpływa na powtarzające się nieukończenie szkoleń, uprzywilejowany dostęp do PII, przetwarzanie PII o istotnym wpływie lub dowody przedstawiane organom regulacyjnym.

9.1.5 [All] Privacy Lead / PIMS Manager musi określić w REG12 właściciela wyjątku, datę wygaśnięcia, działanie kompensujące i datę przeglądu przed zatwierdzeniem jakiegokolwiek wyjątku dotyczącego szkolenia z zakresu prywatności.

9.1.6 [All] Process Owner / Business Owner musi zamknąć albo odnowić zatwierdzone wyjątki dotyczące szkoleń z zakresu prywatności w REG12 przed datą wygaśnięcia wyjątku.

10. Egzekwowanie

10.1.1 [All] Privacy Lead / PIMS Manager musi zarejestrować niezgodność szkoleniową w REG12 w ciągu pięciu dni roboczych, gdy dowody obowiązkowego szkolenia z zakresu prywatności są brakujące, niekompletne, przeterminowane lub nie można ich prześledzić do REG11.

10.1.2 [All] Process Owner / Business Owner musi zapewnić, aby przeterminowane obowiązkowe szkolenie z zakresu prywatności zostało ukończone albo eskalowane w REG11 lub REG12 w ciągu 10 dni roboczych od zarejestrowania statusu przeterminowania.

10.1.3 [Conditional] System Owner / Application Owner musi ograniczyć w REG12 nowy dostęp do PII o istotnym wpływie, gdy wymagane szkolenie wdrożeniowe lub szkolenie z zakresu prywatności oparte na rolach pozostaje nieukończone po eskalacji.

10.1.4 [Processor] Vendor / Procurement Owner musi eskalować brakujące dowody potwierdzające realizację szkoleń podmiotu przetwarzającego, podwykonawcy przetwarzania lub zewnętrznego personelu w REG08 i REG12 w ciągu pięciu dni roboczych od identyfikacji.

10.1.5 [Conditional] Incident Response Coordinator musi powiązać działania egzekwujące dotyczące szkoleń z REG10 w ciągu jednego dnia roboczego, gdy niepowodzenie szkolenia przyczyniło się do podejrzewanego lub potwierdzonego incydentu PII.

10.1.6 [All] Internal Audit / Compliance Reviewer musi zweryfikować dowody zamknięcia działań korygujących dotyczących szkoleń w REG12 podczas kolejnego zaplanowanego audytu albo w ciągu 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1.1 [All] Privacy Lead / PIMS Manager musi dokonywać przeglądu niniejszej polityki i treści szkoleń co najmniej raz w roku oraz rejestrować wynik przeglądu w REG11 lub REG12.

11.1.2 [All] Privacy Lead / PIMS Manager musi dokonać przeglądu niniejszej polityki w ciągu 30 dni po istotnej zmianie zakresu PIMS, prawa dotyczącego prywatności, czynności przetwarzania, modelu ról, wniosków z incydentów, ustaleń z audytu lub wyników skuteczności szkoleń.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor musi dokonać w REG12 przeglądu istotnych dla prywatności zmian polityki przed zatwierdzeniem.

11.1.4 [All] Top Management musi zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.5 [All] Privacy Lead / PIMS Manager musi zaktualizować w REG11 treść szkoleń i dowody przypisania w ciągu 30 dni po zatwierdzonej istotnej zmianie polityki.

12. Powiązane polityki

12.1 Niniejszą politykę należy czytać łącznie z:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności;

12.3 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności;

12.4 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej;

12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości;

12.6 PII05 - Polityka zarządzania zgodami i preferencjami;

12.7 PII06 - Polityka zarządzania prawami osób, których dane dotyczą;

12.8 PII07 - Polityka oceny ryzyka dla prywatności i DPIA;

12.9 PII08 - Polityka privacy by design i privacy by default;

12.10 PII09 - Polityka zbierania, wykorzystywania, ujawniania i udostępniania PII;

12.11 PII10 - Polityka retencji, usuwania i utylizacji PII;

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

12.13 PII13 - Polityka międzynarodowych transferów PII;

12.14 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu;

12.15 PII15 - Polityka zarządzania incydentami i naruszeniami PII;

12.16 PII17 - Polityka zarządzania udokumentowanymi informacjami i dowodami PIMS;

12.17 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS.

13. Normy i ramy odniesienia

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3;

6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].