					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII08					Tytuł dokumentu: **Polityka privacy by design i privacy by default**							
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 6.1.2; Clause 6.1.3	Both	Supporting	Powiązanie oceny ryzyka dla prywatności i postępowania z ryzykiem dla prywatności
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Planowane zmiany i kontrola operacyjna
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Udokumentowane dowody uwzględnienia ochrony danych w fazie projektowania
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie i działanie korygujące
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Cele, wyzwalacz PIA i zapisy
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Ograniczenie zbierania i przetwarzania
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Cele dotyczące poprawności i minimalizacji
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Deidentyfikacja, projektowanie usuwania i pliki tymczasowe
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Umowa z klientem, wsparcie i zapisy podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Możliwości projektowe podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Cykl życia rozwoju i zasady inżynierskie
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Ograniczenie celu, minimalizacja i rozliczalność

GDPR	Article 24	Controller	Supporting	Środki administratora
GDPR	Article 25	Controller	Primary	Ochrona danych w fazie projektowania i domyślna ochrona danych
GDPR	Article 28	Both	Supporting	Polecenia i wsparcie podmiotu przetwarzającego
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania
GDPR	Article 35	Controller	Supporting	Powiązanie wyzwalacza DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Kontrole prywatności w fazie projektowania
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Cel, zbieranie, minimalizacja i ograniczenie wykorzystania
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Poprawność, rozliczalność i zgodność
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Zasady i środki kontroli ochrony PII

1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące wbudowania privacy by design i privacy by default w nowe i zmieniane czynności przetwarzania PII, projekty, produkty, usługi, systemy, aplikacje, integracje, działania zakupowe oraz zmiany procesów biznesowych w zakresie PIMS.

1.2 Niniejsza polityka ma zastosowanie do kontekstów administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania.

1.3 Obowiązki podmiotu przetwarzającego i podwykonawcy przetwarzania mają zastosowanie, gdy organizacja projektuje, konfiguruje, zmienia lub realizuje przetwarzanie w imieniu klienta, administratora lub nadrzędnego podmiotu przetwarzającego na podstawie udokumentowanych poleceń.

1.4 Niniejsza polityka obejmuje następujące obszary:

1.4.1 wymagania dotyczące prywatności na etapie inicjowania projektu;

1.4.2 środki kontroli projektowej dotyczące celu, minimalizacji danych i ustawień domyślnych;

1.4.3 przegląd uwzględnienia ochrony danych w fazie projektowania przed uruchomieniem produkcyjnym;

1.4.4 przegląd uwzględnienia ochrony danych w fazie projektowania wywołany zmianą;

1.4.5 kontrole privacy by design w procesie zakupowym;

1.4.6 powiązanie z ryzykiem dla prywatności, oceną potrzeby przeprowadzenia DPIA oraz dowodami działań korygujących.

1.5 Niniejsza polityka nie zastępuje następujących polityk:

1.5.1 PII03 w zakresie inwentarza przetwarzania, celów, podstawy prawnej i zapisów ROPA;

1.5.2 PII04 w zakresie treści i publikacji klauzuli informacyjnej;

1.5.3 PII05 w zakresie środków kontroli zgody i preferencji;

1.5.4 PII06 w zakresie obsługi praw osób, których dane dotyczą;

1.5.5 PII07 w zakresie metodyki oceny ryzyka dla prywatności i DPIA;

1.5.6 PII09 w zakresie środków kontroli zbierania, wykorzystania, ujawniania i udostępniania;

1.5.7 PII10 w zakresie wykonania retencji, usuwania i utylizacji;

1.5.8 PII11 w zakresie działań dotyczących poprawności i jakości;

1.5.9 PII12 w zakresie zarządzania cyklem życia podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich;

1.5.10 PII13 w zakresie mechanizmów międzynarodowego przekazywania danych;

1.5.11 PII14 w zakresie bezpieczeństwa PII i działania kontroli dostępu;

1.5.12 PII18 w zakresie monitorowania, audytu, działań korygujących i zarządzania doskonaleniem w całym PIMS.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby wymagania dotyczące prywatności były identyfikowane, wdrażane i potwierdzane dowodami przed rozpoczęciem przetwarzania PII lub jego istotną zmianą oraz aby systemy i procesy były domyślnie konfigurowane tak, by ograniczać zbieranie, wykorzystanie, ekspozycję PII, zależności dotyczące retencji, zależności dotyczące ujawniania oraz identyfikowalność do tego, co jest niezbędne dla udokumentowanego celu.

3. Cele szczegółowe

3.1 Celami niniejszej polityki są:

3.1.1 wbudowanie wymagań dotyczących prywatności w decyzje dotyczące inicjowania projektu, projektowania, zakupów, zmian i uruchomienia produkcyjnego;

3.1.2 zapewnienie, aby projekty przetwarzania PII były powiązane z udokumentowanymi celami i zapisami przetwarzania REG02;

3.1.3 wdrożenie minimalizacji danych i domyślnych ustawień chroniących prywatność przed rozpoczęciem przetwarzania;

3.1.4 zapewnienie uruchamiania oceny ryzyka dla prywatności i oceny potrzeby przeprowadzenia DPIA bez powielania metodyki PII07;

3.1.5 zapewnienie rejestrowania wymagań zakupowych i projektowych dotyczących podmiotów przetwarzających bez powielania zarządzania cyklem życia z PII12;

3.1.6 zapewnienie eskalacji nierozwiązanych problemów projektowych przez REG12;

3.1.7 utrzymywanie gotowych do audytu dowodów projektowych w REG02, REG04, REG08 i REG12.

4. Postanowienia polityki

4.1 Inicjowanie projektu i wymagania dotyczące prywatności

4.1.1 [Both] The Process Owner / Business Owner MUSI zarejestrować wpis dotyczący uwzględnienia ochrony danych w fazie projektowania w REG04 przed rozpoczęciem każdego projektu, produktu, usługi, systemu, aplikacji, integracji lub zmiany procesu biznesowego, które obejmują PII.

4.1.2 [Both] The Process Owner / Business Owner MUSI powiązać każdy wpis dotyczący uwzględnienia ochrony danych w fazie projektowania w REG04 z istniejącą lub roboczą czynnością przetwarzania w REG02 przed zatwierdzeniem wymagań funkcjonalnych.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUSI zarejestrować wymagania administratora dotyczące privacy by design w REG04 przed zatwierdzeniem projektu funkcjonalnego administratora.

4.1.4 [Processor] The Vendor / Procurement Owner MUSI zarejestrować polecenia klienta dotyczące projektowania prywatności oraz umowne ograniczenia projektowe w REG08 przed zatwierdzeniem projektu usługi podmiotu przetwarzającego lub istotnej zmiany usługi.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę w REG04 przed zatwierdzeniem projektu PII o wysokim ryzyku, nowatorskiego, wrażliwego, zautomatyzowanego, realizowanego na dużą skalę lub istotnie zmienionego.

4.1.6 [Both] The Information Security Lead MUSI zarejestrować zależności dotyczące środków kontroli bezpieczeństwa PII, które wspierają projekt prywatności, w REG04 przed zatwierdzeniem architektury.

4.2 Minimalizacja danych i projektowanie domyślnej ochrony prywatności

4.2.1 [Controller] The Process Owner / Business Owner MUSI udokumentować minimalne kategorie PII, kategorie osób, których dane dotyczą, źródła i cele w REG02 i REG04 przed zatwierdzeniem projektu zbierania lub importu.

4.2.2 [Both] The System Owner / Application Owner MUSI skonfigurować domyślne ustawienia przetwarzania na minimalne zbieranie i przetwarzanie PII potrzebne do udokumentowanego celu oraz zarejestrować dowody w REG04 przed uruchomieniem produkcyjnym.

4.2.3 [Controller] The Process Owner / Business Owner MUSI udokumentować opcjonalne pola PII, opcjonalne wybory dotyczące przetwarzania oraz ustawienia domyślnie wyłączone w REG02 i REG04 przed zatwierdzeniem interfejsu użytkownika, formularza lub przepływu pracy.

4.2.4 [Both] The System Owner / Application Owner MUSI udokumentować domyślne ustawienia ekspozycji prywatności dla widoków, raportów, eksportów, interfejsów i zautomatyzowanych przepływów pracy w REG04 przed uruchomieniem produkcyjnym.

4.2.5 [Both] The Process Owner / Business Owner MUSI udokumentować wykonalność deidentyfikacji, pseudonimizacji, agregacji lub przetwarzania nieidentyfikowalnego w REG04 przed zatwierdzeniem możliwych do zidentyfikowania PII do testowania, analityki, raportowania lub wtórnego wykorzystania operacyjnego.

4.2.6 [Both] The System Owner / Application Owner MUSI udokumentować postępowanie z tymczasowymi artefaktami PII, w tym plikami tymczasowymi, plikami cache, logami lub zapisami stagingowymi, w REG04 przed uruchomieniem produkcyjnym.

4.2.7 [Both] The Process Owner / Business Owner MUSI skierować wymagania projektowe należące do PII10, PII11, PII13 lub PII14 na powiązaną ścieżkę dowodową polityki w REG04 w ciągu pięciu dni roboczych od zidentyfikowania zależności.

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

9. Wyjątki

9.1 Wyjątki dotyczące projektowania prywatności

9.1.1 [Both] The Process Owner / Business Owner MUSI złożyć wniosek o wyjątek dotyczący projektowania prywatności w REG12 przed zatwierdzeniem projektu lub zmiany, które nie mogą spełnić mającego zastosowanie wymagania dotyczącego projektowania prywatności.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUSI ocenić wpływ, środki kompensujące i datę wygaśnięcia każdego wyjątku dotyczącego projektowania prywatności w REG12 w ciągu pięciu dni roboczych od złożenia wniosku.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę w REG12 przed zatwierdzeniem wyjątku dotyczącego projektowania prywatności obejmującego przetwarzanie o wysokim ryzyku, wrażliwe, zautomatyzowane, realizowane na dużą skalę, sporne lub istotne prawnie.

9.1.4 [All] Top Management MUSI zatwierdzić wyjątek dotyczący projektowania prywatności wpływający na przetwarzanie o wysokim wpływie, zakres certyfikacji, nierozwiązane istotne ryzyko lub obowiązek prawny w REG12 przed wejściem wyjątku w życie.

9.1.5 [Both] The Privacy Lead / PIMS Manager MUSI ustalić datę wygaśnięcia nieprzekraczającą 90 dni w REG12 dla każdego zatwierdzonego wyjątku dotyczącego projektowania prywatności przed zatwierdzeniem.

9.1.6 [Both] The Privacy Lead / PIMS Manager MUSI zamknąć lub ponownie ocenić każdy wyjątek dotyczący projektowania prywatności w REG12 w ciągu pięciu dni roboczych od jego wygaśnięcia.

10. Egzekwowanie postanowień

10.1 Egzekwowanie postanowień i obsługa niezgodności

10.1.1 [Both] The Privacy Lead / PIMS Manager MUSI zarejestrować brak przeglądu projektu prywatności, brak dowodów minimalizacji, nierozwiązaną nieskuteczność ustawień domyślnych lub nieautoryzowane uruchomienie produkcyjne jako niezgodność w REG12 w ciągu pięciu dni roboczych od zidentyfikowania.

10.1.2 [Both] The System Owner / Application Owner MUSI zapobiec uruchomieniu produkcyjnemu systemu przetwarzającego PII, jeżeli przegląd projektu prywatności w REG04 jest niekompletny, oraz zarejestrować decyzję w REG12 przed uruchomieniem produkcyjnym.

10.1.3 [Both] The Vendor / Procurement Owner MUSI zapobiec onboardingowi dostawcy lub podpisaniu umowy, jeżeli brakuje wymaganych dowodów projektowania prywatności w REG08, oraz zarejestrować decyzję w REG12 przed onboardingiem lub podpisaniem.

10.1.4 [Both] The Process Owner / Business Owner MUSI wstrzymać wykorzystanie nowego lub zmienionego projektu przetwarzania PII do czasu ukończenia przeglądu REG04, aktualizacji REG02 i wymaganych wyjątków REG12.

10.1.5 [All] Top Management MUSI wymagać działania korygującego w REG12 w ciągu 10 dni roboczych w przypadku powtarzającej się, przedłużającej się lub wywierającej wysoki wpływ nieskuteczności projektowania prywatności.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących dla niezgodności dotyczących projektowania prywatności w REG12 podczas następnego zaplanowanego audytu PIMS albo w ciągu 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1 Przegląd polityki i środków kontroli projektowej

11.1.1 [All] The Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 co roku oraz w ciągu 30 dni od istotnej zmiany prawnej, przetwarzania, technologii, zakresu certyfikacji lub środka kontroli PIMS.

11.1.2 [Both] The Process Owner / Business Owner MUSI przeglądać aktywne czynności przetwarzania REG02 pod kątem zmian zależności dotyczących projektowania prywatności co roku oraz w ciągu 30 dni od istotnej zmiany przetwarzania.

11.1.3 [Both] The System Owner / Application Owner MUSI przeglądać dowody konfiguracji privacy by default w REG04 co roku oraz w ciągu 30 dni od istotnej zmiany systemowej.

11.1.4 [Both] The Vendor / Procurement Owner MUSI przeglądać obowiązki dostawców, podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich w zakresie projektowania prywatności w REG08 przed odnowieniem oraz w ciągu 30 dni od istotnej zmiany relacji.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSI przeglądać wpływ istotnych zmian polityki na prywatność w REG12 przed zatwierdzeniem.

11.1.6 [All] Top Management MUSI zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.

12. Powiązane polityki

12.1 PII01 - Polityka systemu zarządzania informacjami o prywatności

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

12.3 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej

12.4 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.5 PII05 - Polityka zarządzania zgodami i preferencjami

12.6 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.7 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.8 PII09 - Polityka zbierania, wykorzystania, ujawniania i udostępniania PII

12.9 PII10 - Polityka retencji, usuwania i utylizacji PII

12.10 PII11 - Polityka poprawności i jakości PII

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

12.12 PII13 - Polityka międzynarodowego przekazywania PII

12.13 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.14 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.15 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest odwzorowana na następujące normy i regulacje. Odwzorowanie 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 6.1.2; Clause 6.1.3** - Odwzorowano na ocenę ryzyka dla prywatności, powiązanie działań postępowania z ryzykiem, analizę zależności projektowych, eskalację i działanie korygujące bez powielania pełnej metodyki oceny ryzyka dla prywatności i DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Odwzorowano na planowane zmiany dotyczące prywatności, inicjowanie projektu, operacyjny przegląd projektu prywatności, kontrolę uruchomienia produkcyjnego oraz przegląd istotnych zmian. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Odwzorowano na udokumentowane dowody uwzględnienia ochrony danych w fazie projektowania przechowywane w REG02, REG04, REG08 i REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Odwzorowano na metryki projektowania prywatności, próbkowanie dowodów, rejestrowanie niezgodności, działanie korygujące i weryfikację skuteczności. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Odwzorowano na dokumentowanie celów przetwarzania, zapisów przetwarzania, powiązania projektowania prywatności oraz wyzwalaczy oceny ryzyka dla prywatności lub oceny potrzeby przeprowadzenia DPIA dla przetwarzania przez administratora. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Odwzorowano na ograniczanie zbierania i przetwarzania PII przez minimalne wymagania danych oparte na celu, domyślnie wyłączone przetwarzanie opcjonalne oraz minimalne domyślne ustawienia przetwarzania. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Odwzorowano na kierowanie zależności dotyczących poprawności, cele minimalizacji, wykonalność deidentyfikacji oraz dowody projektowe minimalizowania możliwych do zidentyfikowania PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Odwzorowano na identyfikację na etapie projektowania deidentyfikacji, zależności dotyczących usuwania, tymczasowych artefaktów PII oraz kierowanie do środków kontroli cyklu życia bez powielania wykonywania retencji lub utylizacji. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Odwzorowano na polecenia klienta dla podmiotu przetwarzającego, informacje wspierające klienta, zapisy projektowe podmiotu przetwarzającego oraz autoryzowane przez klienta zmiany projektu usługi. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Odwzorowano na możliwości projektowe podmiotu przetwarzającego dotyczące plików tymczasowych, zależności zwrotu lub utylizacji oraz zależności kontroli transmisji, rejestrowane jako dowody projektowe bez powielania operacyjnych procedur usuwania lub środków kontroli bezpieczeństwa. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Odwzorowano na wymagania dotyczące prywatności w cyklu życia rozwoju, zasadach inżynierskich, punktach kontrolnych ochrony PII oraz dowodach konfiguracji privacy by default. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Odwzorowano na ograniczenie celu, minimalne projektowanie PII, powiązanie z zapisami przetwarzania, domyślną minimalizację, dowody i rozliczalność. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Odwzorowano na środki administratora, przegląd zarządzania, zatwierdzanie wyjątków, działanie korygujące i utrzymanie polityki dotyczące wdrożenia privacy by design. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Odwzorowano na inicjowanie projektu, wymagania dotyczące prywatności na etapie projektowania, ustawienia privacy by default, minimalizację, kontrole projektowe w zakupach, przegląd przed uruchomieniem produkcyjnym oraz przegląd wywołany zmianą. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Odwzorowano na polecenia dla podmiotu przetwarzającego, wsparcie projektowe podmiotu przetwarzającego, dowody projektowania prywatności po stronie dostawcy oraz autoryzowane przez klienta zmiany projektu. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Odwzorowano na powiązanie z zapisami przetwarzania, aktualizacje REG02, zależności projektowe czynności przetwarzania oraz dowody zapisów przetwarzania. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Odwzorowano na wyzwalacze oceny ryzyka dla prywatności i oceny potrzeby przeprowadzenia DPIA na etapie projektowania, porady w przypadku wysokiego ryzyka oraz kontrole powdrożeniowe bez powielania metodyki DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Odwzorowano na identyfikowanie środków kontroli prywatności na etapie projektowania, powiązanie z ryzykiem dla prywatności oraz dowody projektowe wdrożenia środków kontroli. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Odwzorowano na określenie celu, ograniczenie zbierania, minimalizację danych, ograniczone wykorzystanie i domyślne ustawienia przetwarzania. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Odwzorowano na kierowanie zależności dotyczących poprawności, dowody rozliczalności, monitorowanie projektowania prywatności, audyt i działanie korygujące. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Odwzorowano na zasadność celu, ograniczenie zbierania, minimalizację danych, ograniczenie wykorzystania i ujawniania, zależność dotyczącą retencji, postępowanie z plikami tymczasowymi oraz środki kontroli projektowej zależności dotyczących poprawności. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].