| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Wprowadź tutaj nazwę zarejestrowanej osoby prawnej | | | | | | | |
| Numer dokumentu:<br>PII03 | | | | | Tytuł dokumentu:<br>**Polityka inwentarza przetwarzania PII i podstawy prawnej** | | | | | | | |
| Wersja:<br>1.0 | | Data wejścia w życie:<br>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 | Both | Supporting | Określanie roli PIMS dla czynności przetwarzania |
| ISO/IEC 27701:2025 | Clause 6.1.2 | Both | Supporting | Powiązanie z wyzwalaczem oceny ryzyka dla prywatności |
| ISO/IEC 27701:2025 | Clause 6.1.3 | Both | Supporting | Powiązanie stosowalności środków kontrolnych i SoA |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Primary | Udokumentowane informacje dotyczące inwentarza przetwarzania |
| ISO/IEC 27701:2025 | Clause 8.1 | Both | Primary | Planowanie operacyjne i nadzór nad zapisami przetwarzania |
| ISO/IEC 27701:2025 | Clause 8.2 | Both | Supporting | Powiązanie z operacyjną oceną ryzyka dla prywatności |
| ISO/IEC 27701:2025 | Clause 9.1 | Both | Supporting | Monitorowanie i pomiar inwentarza |
| ISO/IEC 27701:2025 | Clause 10.2 | Both | Supporting | Niezgodności inwentarza i działania korygujące |
| ISO/IEC 27701:2025 | Annex A.1.2.2 | Controller | Primary | Identyfikacja celu przez administratora |
| ISO/IEC 27701:2025 | Annex A.1.2.3 | Controller | Primary | Identyfikacja podstawy prawnej przez administratora |
| ISO/IEC 27701:2025 | Annex A.1.2.6 | Controller | Supporting | Powiązanie z oceną potrzeby przeprowadzenia DPIA |
| ISO/IEC 27701:2025 | Annex A.1.2.8 | Joint Controller | Supporting | Zapisy odpowiedzialności za przetwarzanie po stronie współadministratorów |

| | | | | |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Annex A.1.2.9 | Controller | Primary | Zapisy administratora dotyczące przetwarzania PII |
| ISO/IEC 27701:2025 | Annex A.2.2.2 | Processor | Primary | Zapisy umowy z klientem i polecenia klienta dla podmiotu przetwarzającego |
| ISO/IEC 27701:2025 | Annex A.2.2.3 | Processor | Primary | Zgodność celu podmiotu przetwarzającego z poleceniami klienta |
| ISO/IEC 27701:2025 | Annex A.2.2.7 | Processor | Supporting | Zapisy podmiotu przetwarzającego dotyczące przetwarzania PII |
| GDPR | Article 5(1)(a) | Controller | Supporting | Powiązanie zgodności z prawem, rzetelności i przejrzystości |
| GDPR | Article 5(1)(b) | Controller | Supporting | Ograniczenie celu |
| GDPR | Article 5(1)(c) | Controller | Supporting | Minimalizacja danych |
| GDPR | Article 5(1)(e) | Controller | Supporting | Powiązanie z ograniczeniem przechowywania |
| GDPR | Article 5(2) | Controller | Supporting | Dowody rozliczalności |
| GDPR | Article 6 | Controller | Primary | Zgodność przetwarzania z prawem |
| GDPR | Article 9 | Conditional | Supporting | Warunek przetwarzania szczególnych kategorii danych |
| GDPR | Article 10 | Conditional | Supporting | Warunek przetwarzania danych o wyrokach skazujących i czynach zabronionych |
| GDPR | Article 24 | Controller | Supporting | Odpowiedzialność administratora i środki |
| GDPR | Article 26 | Joint Controller | Supporting | Zapisy uzgodnień współadministratorów |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 28 | Both | Supporting | Zapisy poleceń i umów z podmiotami przetwarzającymi |
| GDPR | Article 30 | Both | Primary | Rejestr czynności przetwarzania |
| GDPR | Article 35 | Controller | Supporting | Powiązanie z oceną potrzeby przeprowadzenia DPIA |
| ISO/IEC 29100:2020 | Clause 5.3 | Both | Supporting | Legalność i określenie celu |
| ISO/IEC 29100:2020 | Clause 5.4 | Both | Supporting | Ograniczenie gromadzenia |
| ISO/IEC 29100:2020 | Clause 5.5 | Both | Supporting | Minimalizacja danych |
| ISO/IEC 29100:2020 | Clause 5.6 | Both | Supporting | Ograniczenie wykorzystania, przechowywania i ujawniania |
| ISO/IEC 29100:2020 | Clause 5.10 | Both | Supporting | Rozliczalność |
| ISO/IEC 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7 | Controller | Supporting | Środki kontrolne ochrony PII dotyczące celu, gromadzenia, minimalizacji, wykorzystania, przechowywania i ujawniania |
| ISO/IEC 29134:2020 | Clause 5.1; Clause 6.2 | Both | Supporting | Powiązanie z korzyściami i wyzwalaczami PIA |

## 1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące utrzymywania inwentarza przetwarzania PII / ROPA oraz dokumentowania podstawy prawnej, celów przetwarzania, ról w przetwarzaniu, kategorii PII, kategorii osób, których dane dotyczą, odbiorców, odniesień do okresów przechowywania, odniesień do transferów, poleceń klienta dla podmiotów przetwarzających, zapisów współadministratorów oraz powiązania z oceną ryzyka dla prywatności.

**1.2 Niniejsza polityka ma zastosowanie do:**

1.2.1 wszystkich czynności przetwarzania PII w zakresie PIMS;

1.2.2 przetwarzania realizowanego jako administrator, współadministrator, podmiot przetwarzający lub podwykonawca przetwarzania;

1.2.3 przetwarzania realizowanego przez procesy biznesowe, systemy, aplikacje, dostawców, podmioty przetwarzające, podwykonawców przetwarzania oraz odbiorców, którym udostępniane są dane;

1.2.4 nowego przetwarzania, istotnie zmienionego przetwarzania oraz przetwarzania wycofanego;

1.2.5 dowodów utrzymywanych w REG02 oraz dowodów wspierających w REG01, REG03, REG04, REG05, REG07, REG08, REG09 i REG12.

1.3 Niniejsza polityka nie zastępuje szczegółowych środków kontrolnych dotyczących klauzul informacyjnych, zgody, metodyki DPIA, wykonywania okresów przechowywania, wyboru mechanizmu transferu międzynarodowego, zawierania umów z podmiotami przetwarzającymi, środków bezpieczeństwa PII ani środków kontrolnych dotyczących udokumentowanych informacji. Wymagania te określono w powiązanych politykach wymienionych w sekcji 12.

1.4 Na potrzeby niniejszej polityki zapis inwentarza przetwarzania oznacza wpis w REG02 opisujący odrębną czynność przetwarzania PII, obejmujący jej cel, rolę, właściciela, kategorie PII, kategorie osób, których dane dotyczą, podstawę prawną lub odniesienie do polecenia klienta, systemy, odbiorców, odniesienie do okresu przechowywania, odniesienie do transferu, status ryzyka dla prywatności oraz status przeglądu.

1.5 Na potrzeby niniejszej polityki istotna zmiana przetwarzania oznacza każdą zmianę celu przetwarzania, podstawy prawnej, roli PIMS, kategorii PII, kategorii osób, których dane dotyczą, odbiorcy, systemu, dostawcy, podwykonawcy przetwarzania, lokalizacji przetwarzania, transferu, reguły okresu przechowywania, klasyfikacji bezpieczeństwa, klauzuli informacyjnej, zależności od zgody, statusu DPIA, polecenia klienta lub zakresu certyfikacji.

## 2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby organizacja mogła identyfikować, dokumentować, uzasadniać, przeglądać i wykazywać czynności przetwarzania PII w zakresie PIMS.

2.2 Niniejsza polityka umożliwia organizacji utrzymywanie kompletnego, aktualnego i gotowego do audytu inwentarza przetwarzania PII, który wspiera zgodne z prawem przetwarzanie, rozliczalność, klauzule informacyjne, zarządzanie zgodą, ocenę ryzyka dla prywatności, ocenę potrzeby przeprowadzenia DPIA, okresy przechowywania, zarządzanie transferami, zarządzanie podmiotami przetwarzającymi oraz monitorowanie PIMS.

## 3. Cele szczegółowe

**3.1 Celami niniejszej polityki są:**

3.1.1 ustanowienie REG02 jako autorytatywnego inwentarza przetwarzania PII oraz obiektu dowodowego ROPA;

3.1.2 zapewnienie, aby każda czynność przetwarzania PII miała odpowiedzialnego właściciela;

3.1.3 rozróżnianie zapisów przetwarzania dotyczących administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania;

3.1.4 dokumentowanie konkretnych celów przetwarzania przed rozpoczęciem przetwarzania;

3.1.5 dokumentowanie podstawy prawnej przetwarzania przez administratora przed rozpoczęciem przetwarzania;

3.1.6 dokumentowanie poleceń klienta dla przetwarzania przez podmiot przetwarzający i podwykonawcę przetwarzania przed rozpoczęciem przetwarzania;

3.1.7 dokumentowanie kategorii PII, kategorii osób, których dane dotyczą, odbiorców, odniesień do okresów przechowywania, odniesień do transferów, systemów oraz relacji z dostawcami;

3.1.8 powiązanie zapisów inwentarza z dowodami dotyczącymi klauzul informacyjnych, zgody, DPIA, ryzyka, dostawców, transferów, środków kontrolnych i audytów, o ile ma to zastosowanie;

3.1.9 zapewnienie, aby zapisy inwentarza przetwarzania były przeglądane, aktualizowane i korygowane w przypadku zmian przetwarzania;

3.1.10 unikanie tworzenia odrębnych rejestrów podstaw prawnych lub inwentarzy przetwarzania poza REG02.

## 4. Postanowienia polityki

### 4.1 Bazowy inwentarz przetwarzania

4.1.1 [Both] Process Owner / Business Owner MUSI utworzyć zapis inwentarza przetwarzania w REG02 przed rozpoczęciem każdej nowej czynności przetwarzania PII.

4.1.2 [Both] Process Owner / Business Owner MUSI zarejestrować wymagane pola REG02 dla każdej czynności przetwarzania przed rozpoczęciem tej czynności.

4.1.3 [Both] Privacy Lead / PIMS Manager MUSI zatwierdzić wymagany zestaw pól REG02 w REG12 przed pierwszym uruchomieniem PIMS, a następnie co roku.

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

4.1.5 [Both] System Owner / Application Owner MUSI powiązać każdy system lub każdą aplikację przetwarzającą PII z odpowiednią czynnością przetwarzania w REG02 przed uruchomieniem produkcyjnym systemu.

4.1.6 [Both] Vendor / Procurement Owner MUSI powiązać każdą relację z podmiotem przetwarzającym, podwykonawcą przetwarzania, udostępnianiem danych stronie trzeciej lub współadministratorem w REG08 z odpowiednią czynnością przetwarzania w REG02 przed zatwierdzeniem umowy lub onboardingiem.

### 4.2 Zapisy celu i podstawy prawnej administratora

4.2.1 [Controller] Process Owner / Business Owner MUSI udokumentować konkretny cel przetwarzania w REG02 przed zebraniem, wykorzystaniem, ujawnieniem lub innym przetwarzaniem PII.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUSI zwalidować podstawę prawną zarejestrowaną w REG02 przed rozpoczęciem przetwarzania przez administratora oraz przed wejściem w życie każdej zmiany celu.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę w REG12 przed zatwierdzeniem nowej podstawy prawnej dla przetwarzania wysokiego ryzyka, szczególnych kategorii PII, danych o wyrokach skazujących lub czynach zabronionych albo istotnie zmienionego przetwarzania przez administratora.

4.2.4 [Controller] Process Owner / Business Owner MUSI powiązać REG02 z REG05, zanim przetwarzanie przez administratora oprze się na zgodzie jako podstawie prawnej.

4.2.5 [Controller] Process Owner / Business Owner MUSI zarejestrować odniesienie do oceny prawnie uzasadnionego interesu w REG04, zanim przetwarzanie przez administratora oprze się na prawnie uzasadnionych interesach.

4.2.6 [Conditional] Process Owner / Business Owner MUSI zarejestrować warunek przetwarzania szczególnych kategorii danych w REG02 przed przetwarzaniem szczególnych kategorii PII.

4.2.7 [Conditional] Privacy Lead / PIMS Manager MUSI zarejestrować podstawę upoważnienia do przetwarzania danych o wyrokach skazujących lub czynach zabronionych w REG02 przed przetwarzaniem takich danych.

4.2.8 [Controller] Process Owner / Business Owner MUSI udokumentować zgodność nowego celu z dotychczasowym celem oraz ocenę ryzyka dla prywatności w REG02 i REG04 przed wykorzystaniem PII do nowego celu, który nie został wcześniej zarejestrowany.

[ ... 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 inwentarza przetwarzania i podstawy prawnej

9.1.1 [All] Process Owner / Business Owner MUSI wystąpić o wyjątek w REG12 przed prowadzeniem czynności przetwarzania PII bez wymaganego pola REG02, zapisu podstawy prawnej, odniesienia do polecenia klienta lub statusu przeglądu.

9.1.2 [All] Privacy Lead / PIMS Manager MUSI ocenić wpływ każdego wyjątku od inwentarza przetwarzania na prywatność, certyfikację i działalność operacyjną w REG12 w ciągu 10 dni roboczych od wniosku.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUSI zarejestrować poradę w REG12 przed zatwierdzeniem każdego wyjątku obejmującego podstawę prawną, szczególne kategorie PII, dane o wyrokach skazujących lub czynach zabronionych, przetwarzanie wysokiego ryzyka, powiązanie z transferem międzynarodowym lub ograniczenie polecenia klienta.

9.1.4 [All] Top Management MUSI zatwierdzić w REG12 wyjątki dotyczące inwentarza przetwarzania przekraczające 30 dni, wpływające na przetwarzanie wysokiego ryzyka lub wpływające na zakres certyfikacji przed wejściem wyjątku w życie.

9.1.5 [All] Privacy Lead / PIMS Manager MUSI ustalić w REG12 datę wygaśnięcia nieprzekraczającą 90 dni dla każdego zatwierdzonego wyjątku dotyczącego inwentarza przetwarzania przed jego zatwierdzeniem.

9.1.6 [All] Process Owner / Business Owner MUSI zamknąć lub ponownie ocenić każdy wyjątek dotyczący inwentarza przetwarzania w REG12 w ciągu pięciu dni roboczych od jego wygaśnięcia.

## 10. Egzekwowanie

### 10.1 Egzekwowanie inwentarza przetwarzania i podstawy prawnej

10.1.1 [All] Privacy Lead / PIMS Manager MUSI zarejestrować brakujące, niedokładne, nieaktualne lub niezatwierdzone dowody inwentarza przetwarzania REG02 jako niezgodność w REG12 w ciągu pięciu dni roboczych od ich identyfikacji.

10.1.2 [Controller] Process Owner / Business Owner MUSI wstrzymać nowe przetwarzanie przez administratora, jeżeli przed uruchomieniem w REG02 brakuje wymaganego celu lub dowodów podstawy prawnej.

10.1.3 [Processor] Process Owner / Business Owner MUSI wstrzymać nowe przetwarzanie przez podmiot przetwarzający, jeżeli przed onboardingiem usługi brakuje wymaganych dowodów polecenia klienta w REG02 lub REG08.

10.1.4 [Both] System Owner / Application Owner MUSI zablokować uruchomienie produkcyjne systemu dla przetwarzania PII, jeżeli przed zatwierdzeniem uruchomienia produkcyjnego brakuje wymaganego powiązania z inwentarzem REG02.

10.1.5 [Both] Vendor / Procurement Owner MUSI zablokować onboarding dostawcy, podmiotu przetwarzającego, podwykonawcy przetwarzania, odbiorcy zewnętrznego lub współadministratora, jeżeli przed zatwierdzeniem umowy brakuje wymaganych dowodów powiązania REG02 i REG08.

10.1.6 [All] Top Management MUSI przeglądać nierozwiązane poważne niezgodności dotyczące inwentarza przetwarzania lub podstawy prawnej w REG12 podczas przeglądu zarządzania.

10.1.7 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących dotyczących niezgodności inwentarza przetwarzania w REG12 podczas następnego zaplanowanego audytu albo w ciągu 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

## 11. Przegląd i utrzymanie

### 11.1 Przegląd i utrzymanie polityki

11.1.1 [All] Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 co roku oraz w ciągu 30 dni od istotnej zmiany wymagań dotyczących inwentarza przetwarzania, podstawy prawnej, polecenia klienta dla podmiotu przetwarzającego, ROPA lub certyfikacji.

11.1.2 [All] Privacy Lead / PIMS Manager MUSI przeglądać minimalne wymagania dotyczące pól REG02 w REG12 co roku oraz w ciągu 30 dni od istotnej zmiany prawnej, regulacyjnej, umownej lub dotyczącej przetwarzania.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSI przeglądać zmiany niniejszej polityki istotne z perspektywy prywatności w REG12 przed ich zatwierdzeniem.

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

11.1.5 [All] Privacy Lead / PIMS Manager MUSI zaktualizować REG03 i REG04 w ciągu 15 dni roboczych po zatwierdzonych zmianach polityki, które zmieniają stosowalność środków kontrolnych lub wymagania dotyczące oceny ryzyka dla prywatności.

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

## 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, odpowiedzialności i rozliczalności w zakresie prywatności

12.4 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.5 PII05 - Polityka zarządzania zgodą i preferencjami

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 przechowywania, usuwania i utylizacji PII

12.10 PII11 - Polityka dokładności i jakości PII

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

12.12 PII13 - Polityka międzynarodowego transferu 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 mapowana 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** - Mapowanie dotyczy określania roli PIMS organizacji dla każdej czynności przetwarzania oraz rozróżniania kontekstów administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Mapowanie dotyczy powiązania z wyzwalaczem oceny ryzyka dla prywatności dla nowych i istotnie zmienionych czynności przetwarzania PII. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Mapowanie dotyczy powiązania czynności przetwarzania ze stosowalnością środków kontrolnych oraz dowodami Deklaracji stosowania PIMS. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Mapowanie dotyczy utrzymywania inwentarza przetwarzania, podstawy prawnej, polecenia klienta dla podmiotu przetwarzającego, przeglądu, wyjątków i zapisów działań korygujących jako nadzorowanych udokumentowanych informacji. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].

13.2.5 **Clause 8.1** - Mapowanie dotyczy planowania operacyjnego i nadzoru nad tworzeniem, walidowaniem, aktualizowaniem, przeglądaniem i wycofywaniem zapisów inwentarza przetwarzania przed rozpoczęciem lub zmianą przetwarzania. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].

13.2.6 **Clause 8.2** - Mapowanie dotyczy powiązania operacyjnej oceny ryzyka dla prywatności z zapisami inwentarza przetwarzania oraz wyzwalaczami istotnych zmian przetwarzania. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Mapowanie dotyczy monitorowania i pomiaru kompletności inwentarza przetwarzania, walidacji podstawy prawnej, powiązania polecenia klienta, statusu przeglądu, powiązania z oceną potrzeby przeprowadzenia DPIA oraz wyjątków z uzgodnień. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.8 **Clause 10.2** - Mapowanie dotyczy obsługi niezgodności inwentarza i podstawy prawnej, wyjątków, działań korygujących, egzekwowania oraz weryfikacji skuteczności. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

13.2.9 **Annex A.1.2.2** - Mapowanie dotyczy identyfikowania i dokumentowania celów przetwarzania przez administratora przed zebraniem, wykorzystaniem, ujawnieniem lub innym przetwarzaniem PII. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Mapowanie dotyczy ustalania, dokumentowania, walidowania i wykazywania podstawy prawnej przetwarzania przez administratora. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].

13.2.11 **Annex A.1.2.6** - Mapowanie dotyczy oceny nowych i istotnie zmienionych czynności przetwarzania przez administratora pod kątem potrzeby przeprowadzenia DPIA. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Mapowanie dotyczy rejestrowania celów przetwarzania przez współadministratorów oraz odniesień do podziału odpowiedzialności. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Mapowanie dotyczy utrzymywania zapisów administratora związanych z przetwarzaniem PII, w tym celów, kategorii, odbiorców, odniesień do okresów przechowywania, transferów, podstawy prawnej, oceny ryzyka, właściciela, statusu oraz dowodów przeglądu. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].

13.2.14 **Annex A.2.2.2** - Mapowanie dotyczy umowy klienta z podmiotem przetwarzającym oraz dowodów udokumentowanego polecenia klienta, w tym przedmiotu, czasu trwania, celu, kategorii PII oraz kategorii osób, których dane dotyczą. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].

13.2.15 **Annex A.2.2.3** - Mapowanie dotyczy zapewnienia, aby cele przetwarzania przez podmiot przetwarzający pozostawały zgodne z udokumentowanymi poleceniami klienta. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].

13.2.16 **Annex A.2.2.7** - Mapowanie dotyczy utrzymywania zapisów podmiotu przetwarzającego związanych z przetwarzaniem PII w imieniu klientów. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

**13.3 GDPR**

13.3.1 **Article 5(1)(a)** - Mapowanie dotyczy celu przetwarzania przez administratora, walidacji podstawy prawnej oraz dowodów rozliczalności przed rozpoczęciem przetwarzania. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].

13.3.2 **Article 5(1)(b)** - Mapowanie dotyczy określenia celu, oceny zgodności celu oraz zapobiegania przetwarzaniu dla nieudokumentowanego nowego celu. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].

13.3.3 **Article 5(1)(c)** - Mapowanie dotyczy rejestrowania kategorii PII, kategorii osób, których dane dotyczą, oraz danych źródłowych przed przetwarzaniem, aby wspierać przegląd minimalizacji. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.3.4 **Article 5(1)(e)** - Mapowanie dotyczy rejestrowania reguły okresu przechowywania lub odniesienia do okresu przechowywania dla każdej czynności przetwarzania. Addressed by clauses [4.4.4; 8.1.6].

13.3.5 **Article 5(2)** - Mapowanie dotyczy dowodów rozliczalności dla inwentarza przetwarzania, walidacji podstawy prawnej, przeglądu, uzgodnień, próbkowania audytowego oraz działań korygujących. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].

13.3.6 Article 6 - Mapowanie dotyczy dokumentowania i walidowania podstawy prawnej przetwarzania przez administratora, w tym powiązania ze zgodą, odniesienia do oceny prawnie uzasadnionego interesu oraz zgodności celu. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].

13.3.7 Article 9 - Mapowanie dotyczy rejestrowania warunku przetwarzania szczególnych kategorii danych oraz porady w zakresie prywatności przed przetwarzaniem szczególnych kategorii PII. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

13.3.8 **Article 10** - Mapowanie dotyczy rejestrowania podstawy upoważnienia do przetwarzania danych o wyrokach skazujących lub czynach zabronionych przed przetwarzaniem. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].

13.3.9 **Article 24** - Mapowanie dotyczy zarządzania po stronie administratora, przeglądu, rozliczalności oraz nadzoru kierownictwa nad inwentarzem przetwarzania i zapisami podstaw prawnych. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].

13.3.10 **Article 26** - Mapowanie dotyczy dowodów celu przetwarzania przez współadministratorów oraz podziału odpowiedzialności. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.3.11 **Article 28** - Mapowanie dotyczy poleceń dla podmiotu przetwarzającego i podwykonawcy przetwarzania, umowy, powiązania relacji oraz środków kontrolnych onboardingu. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].

13.3.12 **Article 30** - Mapowanie dotyczy rejestrów czynności przetwarzania administratora i podmiotu przetwarzającego, w tym celów przetwarzania, kategorii PII, kategorii osób, których dane dotyczą, odbiorców, transferów, odniesień do okresów przechowywania oraz zapisów poleceń klienta. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].

13.3.13 **Article 35** - Mapowanie dotyczy powiązania z oceną potrzeby przeprowadzenia DPIA dla nowych, istotnie zmienionych lub wysokiego ryzyka czynności przetwarzania przez administratora. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.3** - Mapowanie dotyczy legalności celu, określenia celu, powiązania z podstawą prawną oraz dowodów zgodności celu. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Mapowanie dotyczy ograniczenia gromadzenia poprzez dokumentowanie kategorii PII, kategorii osób, których dane dotyczą, źródeł i uzasadnienia przed rozpoczęciem przetwarzania. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Mapowanie dotyczy minimalizacji danych poprzez wymagania dotyczące pól inwentarza, dokumentowanie kategorii, dokumentowanie odbiorców oraz przegląd aktualnych zapisów przetwarzania. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Mapowanie dotyczy ograniczenia wykorzystania, przechowywania, ujawniania i transferu poprzez udokumentowane cele, kategorie odbiorców, odniesienia do okresów przechowywania, powiązanie z transferem oraz środki kontrolne zmiany celu. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Mapowanie dotyczy rozliczalności poprzez własność, zarządzanie inwentarzem, przegląd, uzgodnienia, próbkowanie audytowe, obsługę wyjątków oraz dowody działań korygujących. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapowanie dotyczy środków kontrolnych ochrony PII w zakresie legalności celu, ograniczenia gromadzenia, minimalizacji danych oraz ograniczenia wykorzystania, przechowywania i ujawniania. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

**13.6 ISO/IEC 29134:2020**

13.6.1 **Clause 5.1; Clause 6.2** - Mapowanie dotyczy wykorzystania zmian w inwentarzu przetwarzania jako wyzwalacza oceny ryzyka dla prywatności i oceny potrzeby przeprowadzenia DPIA przed kontynuowaniem nowego lub istotnie zmienionego przetwarzania. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].