					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII06					Tytuł dokumentu: **Polityka zarządzania prawami osób, których dane dotyczą**							
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 7.5; Clause 8.1	Both	Primary	Dowody dotyczące wniosków o realizację praw i kontrola operacyjna
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, niezgodności i działania korygujące
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Obowiązki wobec osób, których dane dotyczą
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Sprzeciw, dostęp, sprostowanie i usunięcie
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Powiadamianie stron trzecich i kopia przetwarzanych PII
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Obsługa wniosków i obowiązki dotyczące zautomatyzowanego podejmowania decyzji
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Rejestry przetwarzania prowadzone przez administratora
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 obowiązków i rejestry podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Wsparcie podmiotu przetwarzającego dla obowiązków wobec osób, których dane dotyczą
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Ochrona zapisów dotyczących wniosków o realizację praw
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Przejrzystość i rozliczalność

GDPR	Article 11; Article 12	Controller	Primary	Identyfikacja, tryby składania wniosków, terminy i nadzór nad odpowiedziami
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Dostęp, sprostowanie i usunięcie
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Ograniczenie, powiadomienie i przenoszalność
GDPR	Article 21; Article 22	Controller	Primary	Sprzeciw i zautomatyzowane podejmowanie decyzji
GDPR	Article 24	Controller	Supporting	Odpowiedzialność administratora i środki
GDPR	Article 26	Joint Controller	Supporting	Podział zadań współadministratorów w zakresie realizacji praw
GDPR	Article 28	Both	Primary	Pomoc podmiotu przetwarzającego przy wnioskach o realizację praw
GDPR	Article 30	Both	Supporting	Powiązanie z rejestrami przetwarzania
GDPR	Article 32	Both	Supporting	Bezpieczna obsługa dowodów dotyczących praw i ujawnień
GDPR	Article 39	Conditional	Supporting	Doradztwo i monitorowanie przez DPO, gdy ma zastosowanie
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Przejrzystość, udział osoby fizycznej, rozliczalność i zgodność
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Udział i dostęp osoby, której dane dotyczą

1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące przyjmowania, walidacji, oceny, realizacji, odmowy realizacji, przedłużania terminów, zamykania, monitorowania i dokumentowania dowodów dotyczących wniosków osób, których dane dotyczą, o realizację praw.

1.2 Niniejsza polityka ma zastosowanie do wniosków składanych przez osoby, których dane dotyczą, lub upoważnionych przedstawicieli, dotyczących dostępu, sprostowania, usunięcia, ograniczenia, przenoszalności, sprzeciwu, zautomatyzowanego podejmowania decyzji, kierowania wycofania zgody, skarg oraz powiązanych zapytań.

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

1.4 Obowiązki podmiotu przetwarzającego i podwykonawcy przetwarzania mają zastosowanie wyłącznie wtedy, gdy organizacja wspiera administratora, klienta lub nadrzędny podmiot przetwarzający na podstawie udokumentowanych poleceń.

1.5 Niniejsza polityka nie zastępuje następujących powiązanych polityk:

1.5.1 PII03 w zakresie inwentarza przetwarzania i zapisów podstaw prawnych;

1.5.2 PII04 w zakresie treści i publikacji klauzul informacyjnych;

1.5.3 PII05 w zakresie realizacji zgód i preferencji;

1.5.4 PII10 w zakresie wykonywania przechowywania, usuwania i utylizacji;

1.5.5 PII11 w zakresie nadzoru nad dokładnością i jakością;

1.5.6 PII12 w zakresie nadzoru nad cyklem życia podmiotów przetwarzających i podwykonawców przetwarzania;

1.5.7 PII15 w zakresie obsługi incydentów i naruszeń.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby wnioski osób, których dane dotyczą, o realizację praw były obsługiwane spójnie, zgodnie z prawem, bezpiecznie, w określonych terminach oraz z dowodami gotowymi do audytu.

2.2 Niniejsza polityka zapewnia, że organizacja może wykazać rozliczalność w zakresie przyjmowania wniosków, weryfikacji tożsamości, oceny, realizacji, odmowy, przedłużenia terminu, współpracy z podmiotami przetwarzającymi, zamknięcia i ciągłego doskonalenia.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 Zapewnienie spójnego przyjmowania i śledzenia wszystkich wniosków osób, których dane dotyczą, o realizację praw.

3.1.2 Weryfikacja tożsamości lub umocowania wnioskodawcy przed ujawnieniem, sprostowaniem, usunięciem, ograniczeniem lub przeniesieniem danych.

3.1.3 Ocena wniosków względem rejestrów przetwarzania, klasyfikacji roli, obowiązków prawnych, wymogów umownych i wykonalności technicznej.

3.1.4 Realizacja zasadnych wniosków w udokumentowanych terminach.

3.1.5 Rejestrowanie dowodów odmowy, częściowej realizacji, przedłużenia terminu i zamknięcia.

3.1.6 Wspieranie obowiązków administratora, gdy organizacja działa jako podmiot przetwarzający lub podwykonawca przetwarzania.

3.1.7 Ochrona zapisów dotyczących wniosków o realizację praw oraz pakietów odpowiedzi przed nieuprawnionym ujawnieniem lub zmianą.

3.1.8 Monitorowanie wyników obsługi wniosków o realizację praw oraz inicjowanie działań korygujących, gdy jest to wymagane.

4. Postanowienia polityki

4.1 Przyjmowanie, rejestrowanie i klasyfikacja

4.1.1 [All] Privacy Lead / PIMS Manager MUSI zarejestrować każdy wniosek osoby, której dane dotyczą, o realizację praw w REG06 w ciągu dwóch dni roboczych od otrzymania.

4.1.2 [All] Privacy Lead / PIMS Manager MUSI sklasyfikować typ każdego wniosku, kanał złożenia wniosku, datę wniosku, odniesienie do tożsamości wnioskodawcy, przypisanego właściciela, wewnętrzny termin realizacji, ustawowy lub umowny termin realizacji oraz aktualny status w REG06 przed rozpoczęciem oceny.

4.1.3 [Controller] Privacy Lead / PIMS Manager MUSI potwierdzić otrzymanie wniosku lub przekazać kolejną wymaganą komunikację wnioskodawcy w ciągu pięciu dni roboczych od przyjęcia i zarejestrować komunikację w REG06.

4.1.4 [Controller] Process Owner / Business Owner MUSI powiązać każdy wniosek z właściwą czynnością przetwarzania w REG02 przed przypisaniem działań realizacyjnych.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUSI zidentyfikować stronę będącą współadministratorem odpowiedzialną za obsługę wniosku w REG02, REG06 lub REG08 przed rozpoczęciem merytorycznej oceny.

4.1.6 [Processor] Privacy Lead / PIMS Manager MUSI zarejestrować każde polecenie klienta dotyczące wniosku osoby, której dane dotyczą, o realizację praw w REG06 i REG08 przed rozpoczęciem działań wspierających.

4.1.7 [Subprocessor] Vendor / Procurement Owner MUSI zarejestrować każde polecenie nadrzędne dotyczące wniosku osoby, której dane dotyczą, o realizację praw w REG06 lub REG08 przed rozpoczęciem działań wspierających podwykonawcy przetwarzania.

4.1.8 [All] Incident Response Coordinator MUSI zarejestrować eskalację REG10 w ciągu jednego dnia roboczego, gdy wniosek o realizację praw wskazuje na możliwy incydent lub naruszenie dotyczące PII.

4.2 Weryfikacja tożsamości, zakres i ocena

4.2.1 [Controller] Privacy Lead / PIMS Manager MUSI zweryfikować tożsamość wnioskodawcy lub umocowanie przedstawiciela w REG06 przed ujawnieniem PII lub dokonaniem żądanej zmiany.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUSI żądać wyłącznie minimalnych dodatkowych informacji potrzebnych do weryfikacji oraz zarejestrować żądanie w REG06, gdy tożsamość lub umocowanie są niewystarczające.

4.2.3 [Controller] Process Owner / Business Owner MUSI zidentyfikować właściwe systemy, zapisy, cele, kategorie PII, odbiorców i ograniczenia okresu przechowywania na podstawie REG02 przed oceną realizacji.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor MUSI przejrzeć wnioski wysokiego ryzyka, sporne, niejasne, nadmierne, powtarzające się, odrzucone lub częściowo zrealizowane w REG06 przed zakomunikowaniem decyzji.

4.2.5 [Controller] System Owner / Application Owner MUSI zweryfikować, że proponowane wyciągi odpowiedzi nie obejmują niepowiązanych PII ani nieuprawnionych danych stron trzecich przed udostępnieniem pakietu odpowiedzi.

4.2.6 [Controller] Information Security Lead MUSI przejrzeć metodę dostarczenia odpowiedzi w REG06 lub REG12 przed ujawnieniem PII o dużej objętości, wrażliwych, szczególnych kategorii lub wysokiego ryzyka.

4.2.7 [Controller] Data Protection Officer / Privacy Advisor MUSI przejrzeć wnioski dotyczące zautomatyzowanego podejmowania decyzji lub profilowania w REG06 i REG04 przed realizacją, odmową lub eskalacją.

4.2.8 [Both] Privacy Lead / PIMS Manager MUSI zarejestrować wynik oceny, właściwy typ wniosku, decyzję, uzasadnienie i następne działanie w REG06 przed realizacją lub odmową.

[... 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 wnioskować o wyjątek w REG12 przed odejściem od zatwierdzonych wymagań dotyczących przyjmowania, weryfikacji, realizacji, odpowiedzi lub zamknięcia wniosków o realizację praw.

9.1.2 [All] Privacy Lead / PIMS Manager MUSI zatwierdzić albo odrzucić każdy wyjątek dotyczący obsługi praw w REG12 przed wdrożeniem.

9.1.3 [Controller] Data Protection Officer / Privacy Advisor MUSI przejrzeć każdy wyjątek obejmujący odmowę, częściową realizację, niepewność tożsamości, wrażliwe PII, zautomatyzowane podejmowanie decyzji, wnioski dotyczące dzieci lub przetwarzanie wysokiego ryzyka przed zatwierdzeniem.

9.1.4 [Both] System Owner / Application Owner MUSI zablokować ujawnienie, sprostowanie, usunięcie, ograniczenie lub eksport, gdy wymagany wyjątek nie został zatwierdzony w REG12 przed działaniem.

9.1.5 [All] Privacy Lead / PIMS Manager MUSI przypisać datę wygaśnięcia, właściciela i kontrolę kompensującą dla każdego zatwierdzonego wyjątku dotyczącego obsługi praw w REG12 przed wejściem wyjątku w życie.

10. Egzekwowanie postanowień polityki

10.1.1 [All] Privacy Lead / PIMS Manager MUSI zarejestrować niezgodność w REG12 w ciągu pięciu dni roboczych od zidentyfikowania zaległego, brakującego, niekompletnego, niezweryfikowanego lub niepopartego dowodami zapisu wniosku o realizację praw.

10.1.2 [Controller] System Owner / Application Owner MUSI wstrzymać ujawnienie odpowiedzi do czasu zarejestrowania w REG06 kontroli tożsamości, umocowania i pakietu odpowiedzi.

10.1.3 [Both] Vendor / Procurement Owner MUSI eskalować brak współpracy podmiotu przetwarzającego, podwykonawcy przetwarzania lub strony trzeciej w REG08 i REG12 w ciągu pięciu dni roboczych od identyfikacji.

10.1.4 [All] Top Management MUSI przypisać właścicielstwo działań korygujących w REG12, gdy nieskuteczności obsługi wniosków o realizację praw są systemowe, powtarzające się lub istotne dla certyfikacji.

10.1.5 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować dowody zamknięcia działań korygujących związanych z prawami w REG12 do przypisanego terminu realizacji.

10.1.6 [All] Incident Response Coordinator MUSI zainicjować przegląd REG10 w ciągu jednego dnia roboczego, gdy niezgodność dotycząca wniosku o realizację praw wskazuje na nieuprawnione ujawnienie, utratę, zmianę, niedostępność lub inny podejrzewany incydent dotyczący PII.

11. Przegląd i utrzymanie

11.1.1 [All] Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę corocznie i rejestrować wynik przeglądu w REG12.

11.1.2 [All] Privacy Lead / PIMS Manager MUSI przejrzeć niniejszą politykę w ciągu 30 dni od istotnej zmiany prawa dotyczącego wniosków o realizację praw, zakresu czynności

przetwarzania, narzędzi do obsługi praw, metody weryfikacji tożsamości, modelu usług podmiotu przetwarzającego lub wymagań certyfikacyjnych PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSI przejrzeć zmiany niniejszej polityki istotne dla prywatności w REG12 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 zarejestrować komunikację zatwierdzonych zmian polityki w REG11 w ciągu 30 dni od publikacji.

12. Powiązane polityki

12.1 Niniejsza polityka jest wspierana przez 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 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.6 PII05 - Polityka zarządzania zgodami i preferencjami

12.7 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.8 PII08 - Polityka privacy by design i privacy by default

12.9 PII09 - Polityka zbierania, wykorzystywania, ujawniania i udostępniania PII

12.10 PII10 - Polityka przechowywania, usuwania i utylizacji PII

12.11 PII11 - Polityka dokładności i jakości PII

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

12.13 PII13 - Polityka międzynarodowego przekazywania PII

12.14 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.15 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII

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

12.17 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.18 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest mapowana do następujących norm i regulacji. 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 7.5; Clause 8.1** - Mapowanie do udokumentowanych zapisów wniosków o realizację praw, operacyjnego przepływu pracy wniosków, weryfikacji tożsamości, realizacji, odpowiedzi, zamknięcia oraz dowodów wsparcia podmiotu przetwarzającego. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapowanie do metryk wniosków o realizację praw, monitorowania zaległych wniosków, próbkowania audytowego, rejestrowania niezgodności, działań korygujących i weryfikacji skuteczności. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Mapowanie do określania i realizacji obowiązków wobec osób, których dane dotyczą, poprzez udokumentowane kategorie praw, kanały przyjmowania, weryfikację,

ocenę, odpowiedź i kryteria zamknięcia. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapowanie do obsługi sprzeciwu, dostępu, sprostowania, usunięcia i ograniczenia, weryfikacji, realizacji oraz obsługi spornej dokładności. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapowanie do powiadamiania stron trzecich po wynikach dotyczących praw oraz dostarczania kopii lub przenośnych pakietów odpowiedzi. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapowanie do udokumentowanej obsługi zasadnych wniosków, terminów, przedłużeń, odmowy, zamknięcia oraz przeglądu wniosków dotyczących zautomatyzowanego podejmowania decyzji. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Mapowanie do powiązania wniosków o realizację praw z rejestrami przetwarzania, celami przetwarzania, systemami, kategoriami, odbiorcami i ograniczeniami okresu przechowywania. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapowanie do poleceń wynikających z umowy z klientem, wsparcia podmiotu przetwarzającego dla obowiązków klienta oraz rejestrów podmiotu przetwarzającego dotyczących działań wsparcia praw. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Mapowanie do środków podmiotu przetwarzającego służących wspieraniu obowiązków administratora wobec osób, których dane dotyczą, w tym wsparcia pobierania, sprostowania, ograniczenia, usuwania i eksportu na podstawie udokumentowanego polecenia. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Mapowanie do ochrony zapisów dotyczących wniosków o realizację praw, bezpiecznej obsługi pakietów odpowiedzi, kontroli dostarczania odpowiedzi i ochrony dowodów zamknięcia. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(2)** - Mapowanie do przejrzystej obsługi praw, dowodów rozliczalności, rejestrów wniosków, zapisów odpowiedzi, próbkowania audytowego i działań korygujących. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Mapowanie do identyfikacji, dodatkowych informacji, gdy są konieczne, terminów odpowiedzi, komunikacji, przedłużenia, odmowy i zamknięcia wniosku. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Mapowanie do wyników wyszukiwania dostępu, sprostowania, usunięcia, weryfikacji, dowodów realizacji i dostarczenia pakietu odpowiedzi. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Mapowanie do ograniczenia, powiadamiania właściwych stron o wynikach dotyczących praw oraz przenoszalności lub dostarczania kopii. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Mapowanie do oceny sprzeciwu oraz przeglądu wniosków dotyczących zautomatyzowanego podejmowania decyzji lub profilowania. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Mapowanie do środków nadzoru administratora, ról, właścicielstwa przepływu pracy, przeglądu, wyjątków, działań korygujących i nadzoru kierownictwa nad obsługą praw. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mapowanie do identyfikowania odpowiedzialności współadministratora za obsługę wniosków przed rozpoczęciem merytorycznej oceny. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mapowanie do pomocy podmiotu przetwarzającego i podwykonawcy przetwarzania, udokumentowanych poleceń klienta, terminów wsparcia, braku bezpośredniej odpowiedzi bez upoważnienia oraz eskalacji braku współpracy. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mapowanie do powiązania wniosków o realizację praw z rejestrami przetwarzania, czynnościami przetwarzania, systemami, kategoriami PII, odbiorcami i rejestrami podmiotu przetwarzającego. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mapowanie do bezpiecznej obsługi wniosków o realizację praw, ochrony dostarczania odpowiedzi, zapobiegania nieuprawnionemu ujawnieniu i ochrony dowodów dotyczących praw. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mapowanie do doradztwa i monitorowania przez Data Protection Officer / Privacy Advisor w odniesieniu do wniosków o realizację praw wysokiego ryzyka, spornych, odrzuconych, przedłużonych i związanych ze zautomatyzowanym podejmowaniem decyzji. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapowanie do przejrzystości kanałów realizacji praw, udziału osoby fizycznej i dostępu, rozliczalności, procedur skargowych i dochodzenia roszczeń, monitorowania zgodności z prywatnością oraz dowodów audytowych. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Mapowanie do udziału i dostępu osoby, której dane dotyczą, weryfikacji tożsamości, dostępu, sprostowania, usunięcia, aktualizacji statusu, wsparcia podmiotu przetwarzającego oraz mechanizmów skargowych i dochodzenia roszczeń. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Wymagania wewnętrzne

13.6.1 Wymaganie wewnętrzne - Klauzule określające REG06 jako podstawowy obiekt dowodowy dotyczący praw, szkolenia, zatwierdzanie niestandardowego przepływu pracy, wygaśnięcie wyjątku, przegląd polityki i komunikację zmian polityki wspierają spójność wdrożenia, lecz nie są bezpośrednio mapowane do jednej klauzuli zewnętrznej. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].