					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII07					Tytuł dokumentu: **Polityka oceny ryzyka dla prywatności i DPIA**							
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 6.1.1	Both	Primary	Ryzyka i szanse PIMS
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 powiązanie z SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planowane zmiany PIMS i ponowna ocena ryzyka
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Udokumentowane informacje dotyczące ryzyka dla prywatności i DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	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	Supporting	Monitorowanie i pomiar ryzyka dla prywatności
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Przegląd zarządzania ryzykiem dla prywatności
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Niezgodność związana z ryzykiem oraz działania korygujące
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Ocena skutków dla prywatności
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Rejestry przetwarzania

				wspierające ocenę ryzyka
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Umowa klienta z podmiotem przetwarzającym oraz wsparcie przy DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informacje od podmiotu przetwarzającego wspierające zgodność klienta
GDPR	Article 5(2)	Controller	Supporting	Dowody rozliczalności
GDPR	Article 24	Controller	Supporting	Odpowiedzialność administratora i środki
GDPR	Article 25	Controller	Supporting	Ochrona danych w fazie projektowania i domyślna ochrona danych
GDPR	Article 28	Both	Supporting	Wsparcie podmiotu przetwarzającego i polecenia
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania wspierające DPIA
GDPR	Article 32	Both	Supporting	Ryzyko bezpieczeństwa i środki ochrony
GDPR	Article 35	Controller	Primary	Ocena skutków dla ochrony danych
GDPR	Article 36	Controller	Primary	Uprzednie konsultacje
GDPR	Article 39	Conditional	Supporting	Doradztwo i monitorowanie DPO, gdy ma zastosowanie
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Środki kontrolne prywatności, bezpieczeństwo informacji i zgodność w zakresie prywatności

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Zakres PIA, korzyści, wyzwalacz i przygotowanie
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program ochrony PII i identyfikacja wymagań
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integracja zarządzania organizacyjnym ryzykiem dla prywatności

1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące oceny ryzyka dla prywatności, oceny potrzeby przeprowadzenia DPIA, realizacji pełnej DPIA, postępowania z ryzykiem, akceptacji ryzyka rezydualnego, konsultacji, przeglądu i zarządzania dowodami dla przetwarzania PII w zakresie PIMS.

1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 nowych i istotnie zmienionych czynności przetwarzania PII;

1.2.2 kontekstów przetwarzania jako administrator, współadministrator, podmiot przetwarzający i podwykonawca przetwarzania;

1.2.3 systemów, aplikacji, usług, procesów biznesowych, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania, transferów międzynarodowych oraz uzgodnień dotyczących udostępniania danych, które wpływają na przetwarzanie PII;

1.2.4 dowodów dotyczących ryzyka dla prywatności i DPIA utrzymywanych w REG04 oraz dowodów wspierających utrzymywanych w REG02, REG03, REG08, REG09, REG10, REG11 i REG12.

1.3 Niniejsza polityka nie zastępuje środków kontrolnych dotyczących inwentaryzacji przetwarzania, klauzul informacyjnych, zgody, praw osób, których dane dotyczą, privacy by design, dostawców, transferów międzynarodowych, bezpieczeństwa PII, incydentów, udokumentowanych informacji ani monitorowania/audytu/doskonalenia. Wymagania te określono w powiązanych politykach wskazanych w sekcji 12.

1.4 Na potrzeby niniejszej polityki ocena ryzyka dla prywatności oznacza udokumentowaną identyfikację, analizę, ocenę, postępowanie z ryzykiem, przegląd i monitorowanie potencjalnych negatywnych skutków dla prywatności wynikających z przetwarzania PII.

1.5 Na potrzeby niniejszej polityki DPIA oznacza udokumentowaną ocenę stosowaną dla przetwarzania realizowanego przez administratora, które może powodować wysokie ryzyko dla osób, których dane dotyczą, i która ocenia niezbędność przetwarzania, proporcjonalność, ryzyka, środki ochrony, ryzyko rezydualne, potrzeby konsultacyjne oraz warunki zatwierdzenia.

1.6 Na potrzeby niniejszej polityki wysokie ryzyko rezydualne dla prywatności oznacza ryzyko dla prywatności, które po zaproponowanym lub wdrożonym postępowaniu z ryzykiem pozostaje powyżej zatwierdzonego progu akceptacji.

1.7 Na potrzeby niniejszej polityki istotna zmiana oznacza każdą zmianę wpływającą na zakres PIMS, cel przetwarzania, podstawę prawną, kategorie PII, kategorie osób, których dane dotyczą, skalę przetwarzania, technologię przetwarzania, monitorowanie lub profilowanie, zautomatyzowane podejmowanie decyzji, osoby, których dane dotyczą, wymagające szczególnej ochrony, odbiorców, podmioty przetwarzające, podwykonawców przetwarzania, transfery międzynarodowe, okres przechowywania, środki bezpieczeństwa, profil ryzyka, polecenia klienta lub zakres certyfikacji.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby ryzyka dla prywatności i obowiązki związane z DPIA były identyfikowane, oceniane, obejmowane postępowaniem z ryzykiem, zatwierdzane, przeglądane i dokumentowane dowodowo, zanim przetwarzanie PII spowoduje nieakceptowalne ryzyko dla osób, których dane dotyczą, lub dla PIMS.

2.2 Niniejsza polityka umożliwia organizacji wykazanie zarządzania prywatnością opartego na ryzyku, rozliczalności administratora w zakresie DPIA, wsparcia DPIA przez podmiot przetwarzający, udokumentowanego postępowania z ryzykiem, zatwierdzenia ryzyka rezydualnego, podejmowania decyzji o uprzednich konsultacjach oraz ciągłego doskonalenia środków kontrolnych prywatności.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 określenie obowiązkowych wyzwalaczy wstępnej oceny ryzyka dla prywatności;

3.1.2 określenie, kiedy wymagana jest pełna DPIA;

3.1.3 zapewnienie, aby decyzje administratora dotyczące DPIA były dokumentowane i możliwe do przeglądu;

3.1.4 zapewnienie, aby wsparcie DPIA udzielane przez podmiot przetwarzający i podwykonawcę przetwarzania było dokumentowane, gdy wymagają tego polecenie klienta lub umowa;

3.1.5 zapewnienie, aby ryzyka dla prywatności były oceniane przed rozpoczęciem nowego lub istotnie zmienionego przetwarzania PII;

3.1.6 zapewnienie, aby działania w zakresie postępowania z ryzykiem dla prywatności były przypisywane, wdrażane i weryfikowane;

3.1.7 zapewnienie eskalacji i zatwierdzania wysokiego ryzyka rezydualnego dla prywatności przed rozpoczęciem lub kontynuacją przetwarzania;

3.1.8 zapewnienie dokumentowania decyzji o uprzednich konsultacjach, gdy utrzymuje się wysokie ryzyko rezydualne;

3.1.9 zapewnienie utrzymywania dowodów dotyczących ryzyka dla prywatności i DPIA w REG04 oraz powiązania ich z odpowiednimi obiektami dowodowymi;

3.1.10 unikanie tworzenia odrębnych rejestrów DPIA, ryzyka lub konsultacji poza REG04.

4. Postanowienia polityki

4.1 Wstępna ocena ryzyka dla prywatności

4.1.1 [Both] Process Owner / Business Owner musi zainicjować wstępną ocenę ryzyka dla prywatności w REG04 przed rozpoczęciem nowego lub istotnie zmienionego przetwarzania PII zarejestrowanego w REG02.

4.1.2 [Both] Privacy Lead / PIMS Manager musi utrzymywać kryteria wstępnej oceny ryzyka dla prywatności w REG04 przed pierwszym uruchomieniem PIMS, a następnie corocznie.

4.1.3 [Controller] Process Owner / Business Owner musi przeprowadzić ocenę potrzeby przeprowadzenia DPIA w REG04 przed rozpoczęciem przetwarzania przez administratora spełniającego kryteria wstępnej oceny ryzyka dla prywatności.

4.1.4 [Processor] Vendor / Procurement Owner musi zarejestrować wymagania klienta dotyczące wsparcia DPIA w REG08 przed rozpoczęciem przetwarzania przez podmiot przetwarzający, gdy umowa z klientem lub udokumentowane polecenie wymagają wsparcia DPIA.

4.1.5 [Both] System Owner / Application Owner musi dostarczyć w REG04 dowody dotyczące projektu systemu, dostępu, bezpieczeństwa, rejestrowania i przepływów danych przed zatwierdzeniem oceny ryzyka dla prywatności dla nowych lub istotnie zmienionych systemów przetwarzających PII.

4.1.6 [Both] Privacy Lead / PIMS Manager musi zarejestrować wynik wstępnej oceny oraz uzasadnienie decyzji dotyczącej pełnej DPIA w REG04 przed kontynuowaniem czynności przetwarzania.

4.2 Wyzwalacze DPIA i ustalenie wymogu

4.2.1 [Controller] Privacy Lead / PIMS Manager musi wymagać pełnej DPIA w REG04 przed rozpoczęciem przetwarzania przez administratora, które może powodować wysokie ryzyko.

4.2.2 [Controller] Process Owner / Business Owner musi skierować do Privacy Lead / PIMS Manager w REG04, przed rozpoczęciem przetwarzania, przetwarzanie obejmujące dużą skalę, systematyczne monitorowanie, profilowanie, zautomatyzowane decyzje, szczególne kategorie

PII, dane dotyczące wyroków skazujących lub czynów zabronionych, osoby, których dane dotyczą, wymagające szczególnej ochrony, innowacyjną technologię lub istotnie zmienione przetwarzanie.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor musi zarejestrować poradę w REG04 przed zatwierdzeniem decyzji o wymogu pełnej DPIA dla przetwarzania wysokiego ryzyka przez administratora.

4.2.4 [Both] Process Owner / Business Owner musi ponownie przeprowadzić wstępną ocenę ryzyka dla prywatności w REG04 przed wykorzystaniem PII do nowego celu, dodaniem nowego odbiorcy, wprowadzeniem nowego podmiotu przetwarzającego lub podwykonawcy przetwarzania, zmianą architektury systemu lub rozpoczęciem nowego transferu międzynarodowego.

4.2.5 [Processor] Privacy Lead / PIMS Manager musi udokumentować w REG08, czy wymagane jest wsparcie DPIA przez podmiot przetwarzający, w terminie 10 dni roboczych od otrzymania żądania klienta dotyczącego wsparcia DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner musi udokumentować wymagania dotyczące wsparcia DPIA wynikające z relacji nadrzędnej w REG08 przed rozpoczęciem podprzetwarzania, gdy klient nadrzędny lub umowa z podmiotem przetwarzającym wymagają takiego wsparcia.

[... 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 ryzyka dla prywatności i DPIA

9.1.1 [All] Process Owner / Business Owner musi wnioskować o każdy wyjątek od niniejszej polityki w REG12 przed wystąpieniem odstępstwa.

9.1.2 [All] Privacy Lead / PIMS Manager musi ocenić wpływ każdego wnioskowanego wyjątku na prywatność, kwestie prawne, certyfikację, operacje oraz osoby, których dane dotyczą, w REG04 lub REG12 w terminie 10 dni roboczych od wniosku.

9.1.3 [All] Data Protection Officer / Privacy Advisor musi zarejestrować poradę w REG12 przed zatwierdzeniem każdego wyjątku wpływającego na przetwarzanie wysokiego ryzyka, ukończenie pełnej DPIA, uprzednie konsultacje, wysokie ryzyko rezydualne dla prywatności lub wsparcie DPIA dla klienta.

9.1.4 [All] Top Management musi zatwierdzić wyjątki dotyczące ryzyka dla prywatności lub DPIA, które wpływają na przetwarzanie wysokiego ryzyka, zakres certyfikacji, uprzednie konsultacje lub nierozwiązane wysokie ryzyko rezydualne dla prywatności, w REG12 przed wejściem wyjątku w życie.

9.1.5 [All] Privacy Lead / PIMS Manager musi przed zatwierdzeniem ustalić w REG12 datę wygaśnięcia nieprzekraczającą 90 dni dla każdego zatwierdzonego wyjątku dotyczącego ryzyka dla prywatności lub DPIA.

9.1.6 [All] Process Owner / Business Owner musi zamknąć lub ponownie ocenić każdy wyjątek dotyczący ryzyka dla prywatności lub DPIA w REG12 w terminie pięciu dni roboczych od jego wygaśnięcia.

10. Egzekwowanie

10.1 Egzekwowanie wymagań dotyczących ryzyka dla prywatności i DPIA

10.1.1 [All] Privacy Lead / PIMS Manager musi zarejestrować brakujące, niedokładne, niekompletne, opóźnione lub niezatwierdzone dowody ryzyka dla prywatności lub DPIA w REG04 jako niezgodność w REG12 w terminie pięciu dni roboczych od identyfikacji.

10.1.2 [Controller] Process Owner / Business Owner musi zawiesić nowe przetwarzanie wysokiego ryzyka przez administratora, gdy przed uruchomieniem brakuje wymaganych dowodów zatwierdzenia DPIA w REG04.

10.1.3 [Both] System Owner / Application Owner musi zablokować uruchomienie produkcyjne systemów przetwarzających PII, gdy przed zatwierdzeniem uruchomienia produkcyjnego brakuje wymaganych dowodów postępowania z ryzykiem w REG04.

10.1.4 [Both] Vendor / Procurement Owner musi zablokować onboarding dostawcy, podmiotu przetwarzającego, podwykonawcy przetwarzania lub uzgodnienia dotyczącego udostępniania danych, gdy przed zatwierdzeniem umowy brakuje wymaganych dowodów ryzyka dla prywatności lub wsparcia DPIA w REG04.

10.1.5 [All] Top Management musi przeglądać nierozwiązane istotne niezgodności dotyczące ryzyka dla prywatności lub DPIA w REG12 podczas przeglądu zarządzania.

10.1.6 [All] Privacy Lead / PIMS Manager musi eskalować powtarzające się niedotrzymanie terminów wstępnej oceny REG04, przeglądu DPIA lub postępowania z ryzykiem do Top Management w REG12 w terminie pięciu dni roboczych po drugim wystąpieniu w okresie 12 miesięcy.

10.1.7 [All] Internal Audit / Compliance Reviewer musi zweryfikować skuteczność działań korygujących dotyczących niezgodności w zakresie ryzyka dla prywatności i DPIA w REG12 podczas następnego zaplanowanego audytu albo w terminie 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 corocznie oraz w terminie 30 dni od istotnej zmiany wymagań dotyczących ryzyka dla prywatności, DPIA, uprzednich konsultacji, wsparcia podmiotu przetwarzającego lub certyfikacji dokonywać przeglądu niniejszej polityki w REG12.

11.1.2 [All] Privacy Lead / PIMS Manager musi corocznie przeglądać w REG12 kryteria wstępnej oceny REG04, kryteria obowiązku przeprowadzenia DPIA, kryteria poziomu ryzyka oraz kryteria akceptacji ryzyka rezydualnego.

11.1.3 [All] Data Protection Officer / Privacy Advisor musi przeglądać w REG12 zmiany niniejszej polityki istotne z punktu widzenia prywatności przed ich 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 REG03 i REG04 w terminie 15 dni roboczych po zatwierdzeniu zmian polityki, które zmieniają stosowalność środków kontrolnych, kryteria ryzyka lub wymagania dotyczące oceny potrzeby przeprowadzenia DPIA.

11.1.6 [All] Privacy Lead / PIMS Manager musi zarejestrować komunikację zatwierdzonych zmian niniejszej polityki w REG11 w terminie 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 obszarze 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 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

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 międzynarodowych transferów PII

12.14 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.15 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII

12.16 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.17 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 cytowane wymagania, oraz wskazuje klauzule wewnętrzne, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Mapowanie dotyczy identyfikowania i planowania działań dla ryzyk i szans PIMS z wykorzystaniem kryteriów wstępnej oceny, progów ryzyka, eskalacji oraz danych wejściowych do przeglądu zarządzania. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapowanie dotyczy przeprowadzania wstępnej oceny ryzyka dla prywatności, oceny ryzyka dla prywatności, oceny poziomu ryzyka, ponownej oceny oraz oceny wyzwalaczy DPIA przed kontynuacją nowego lub istotnie zmienionego przetwarzania. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapowanie dotyczy planowania postępowania z ryzykiem dla prywatności, aktualizacji stosowalności środków kontrolnych, wdrożenia postępowania z ryzykiem, akceptacji ryzyka rezydualnego oraz powiązania z SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapowanie dotyczy planowanych zmian PIMS i zmian przetwarzania wyzwalających ponowną ocenę ryzyka dla prywatności oraz przegląd DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapowanie dotyczy nadzorowanych udokumentowanych informacji dla wstępnej oceny ryzyka dla prywatności, dowodów DPIA, postępowania z ryzykiem, akceptacji ryzyka rezydualnego, decyzji o uprzednich konsultacjach, wyjątków, niezgodności oraz dowodów przeglądu polityki. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapowanie dotyczy stosowania środków kontroli ryzyka dla prywatności i DPIA przed uruchomieniem produkcyjnym, onboardingiem, zatwierdzeniem przetwarzania, zamknięciem postępowania z ryzykiem oraz powiązaniem z działaniami korygującymi. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapowanie dotyczy operacyjnej oceny ryzyka dla prywatności dla nowych, zmienionych, systemowych, dostawczych, transferowych i incydentowych zmian przetwarzania. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapowanie dotyczy operacyjnego postępowania z ryzykiem dla prywatności, przypisywania postępowania z ryzykiem, wdrażania postępowania z ryzykiem, eskalacji

opóźnionego postępowania z ryzykiem oraz weryfikacji skuteczności. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapowanie dotyczy monitorowania i pomiaru pokrycia wstępną oceną, statusu DPIA, otwartych ryzyk, opóźnionych działań w zakresie postępowania z ryzykiem, działań dostawców, działań w zakresie postępowania z ryzykiem bezpieczeństwa, działań ponownej oceny po incydentach oraz ustaleń z audytu. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapowanie dotyczy przeglądu zarządzania wysokimi ryzykami rezydualnymi dla prywatności, opóźnionymi działaniami w zakresie postępowania z ryzykiem, statusem pełnych DPIA, decyzjami o uprzednich konsultacjach oraz istotnymi wyjątkami dotyczącymi ryzyka dla prywatności. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapowanie dotyczy niezgodności i wyjątków dotyczących ryzyka dla prywatności i DPIA, otwierania działań korygujących, eskalacji oraz weryfikacji skuteczności. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapowanie dotyczy oceny potrzeby oraz, w stosownych przypadkach, realizacji oceny skutków dla prywatności dla nowego lub zmienionego przetwarzania przez administratora. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapowanie dotyczy rejestrów przetwarzania wspierających dane wejściowe do oceny ryzyka dla prywatności i DPIA, w tym celu, kategorii, systemów, odbiorców, transferów i dostawców. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapowanie dotyczy umów klientów z podmiotami przetwarzającymi oraz obowiązków wsparcia DPIA dla klienta. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapowanie dotyczy przekazywania przez podmiot przetwarzający informacji potrzebnych do zgodności klienta, w tym wsparcia DPIA i dowodów wsparcia klienta. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapowanie dotyczy dowodów rozliczalności dla oceny potrzeby przeprowadzenia DPIA, decyzji dotyczących pełnej DPIA, postępowania z ryzykiem, akceptacji ryzyka rezydualnego, decyzji o uprzednich konsultacjach, wyjątków, ustaleń z audytu oraz działań korygujących. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapowanie dotyczy odpowiedzialności administratora za odpowiednie środki ryzyka dla prywatności, przegląd wysokiego ryzyka rezydualnego, zatwierdzenie przez kierownictwo oraz utrzymanie polityki. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapowanie dotyczy dowodów privacy by design i privacy by default wykorzystywanych w ocenie ryzyka oraz przed zatwierdzeniem uruchomienia produkcyjnego. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapowanie dotyczy wsparcia DPIA przez podmiot przetwarzający i podwykonawcę przetwarzania, obsługi poleceń klienta oraz dowodów postępowania z ryzykiem dostawcy. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapowanie dotyczy rejestrów przetwarzania wspierających dane wejściowe do oceny ryzyka dla prywatności i DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapowanie dotyczy danych wejściowych dotyczących ryzyka bezpieczeństwa PII, doboru środków ochrony, postępowania z ryzykiem bezpieczeństwa oraz aktualizacji statusu środków kontrolnych bezpieczeństwa. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapowanie dotyczy oceny potrzeby przeprowadzenia DPIA, ustalenia wymogu pełnej DPIA, treści DPIA, porad DPO, przeglądu oraz blokowania przetwarzania wysokiego ryzyka bez wymaganego zatwierdzenia DPIA. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapowanie dotyczy podejmowania decyzji o uprzednich konsultacjach, porad DPO, zatwierdzenia przez Top Management oraz działań polegających na kontynuacji, zawieszeniu, przeprojektowaniu lub konsultacji, gdy utrzymuje się wysokie ryzyko rezydualne. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapowanie dotyczy porad i monitorowania przez Data Protection Officer / Privacy Advisor, gdy ma zastosowanie, w odniesieniu do decyzji DPIA, przetwarzania wysokiego ryzyka, uprzednich konsultacji i zmian polityki. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapowanie dotyczy identyfikacji środków kontrolnych prywatności, środków ochrony bezpieczeństwa, zgodności w zakresie prywatności, dowodów ryzyka dla prywatności, monitorowania i przeglądu. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapowanie dotyczy zakresu procesu PIA, korzyści, ustalenia wyzwalacza, przygotowania, danych wejściowych do oceny, dowodów interesariuszy oraz struktury raportu DPIA utrzymywanej w REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapowanie dotyczy wymagań programu ochrony PII, identyfikacji wymagań ochrony PII, doboru środków kontrolnych opartego na ryzyku oraz powiązania z postępowaniem z ryzykiem dla prywatności. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapowanie dotyczy zasad organizacyjnego ryzyka dla prywatności, przywództwa, integracji, oceny ryzyka, postępowania z ryzykiem, monitorowania i przeglądu oraz rejestrowania i raportowania. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].