

				Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII22				Tytuł dokumentu: Polityka prywatności w marketingu i plików cookie							
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

Nota prawna (prawa autorskie i ograniczenia użytkowania)
(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.

Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.

W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Applicability	Coverage Type	Komentarz
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Udokumentowane dowody dotyczące prywatności w marketingu oraz 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.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9	Controller	Primary	Cele marketingowe, powiązanie z podstawą prawną, zgoda i rejestry przetwarzania
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Podmioty przetwarzające w marketingu oraz odpowiedzialności współadministratorów
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Klauzule informacyjne dotyczące marketingu, informacje o plikach cookie oraz informacje o wycofaniu zgody
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Obsługa sprzeciwów i kierowanie wniosków dotyczących marketingu bezpośredniego
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Zbieranie, przetwarzanie i minimalizacja danych na potrzeby marketingu i śledzenia
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Kierowanie transferów i ujawnień dotyczących technologii reklamowych (adtech) i analityki

ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Umowa z podmiotem przetwarzającym, polecenia, wsparcie klienta i rejestry podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Wsparcie podmiotu przetwarzającego w zakresie obowiązków oraz kierowanie transferów i ujawnień
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrona zapisów i dowody rejestrowania zmian w śledzeniu
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Rzetelność, przejrzystość, ograniczenie celu, minimalizacja i rozliczalność
GDPR	Article 6; Article 7	Controller	Primary	Zgodność z prawem i warunki zgody
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Przejrzyste informacje i klauzule informacyjne
GDPR	Article 21	Controller	Primary	Sprzeciw wobec marketingu bezpośredniego i kierowanie rezygnacji
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Rozliczalność, privacy by design i privacy by default, współadministratorzy, podmioty przetwarzające, rejestry i wsparcie bezpieczeństwa
GDPR	Article 44	Conditional	Referenced	Kierowanie transferów międzynarodowych dotyczących dostawców marketingowych
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Zgoda i wybór, przejrzystość oraz uczestnictwo

ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Ograniczenie celu, zbierania, minimalizacji, wykorzystywania i ujawniania
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Rozliczalność, bezpieczeństwo informacji i zgodność
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Zgoda, cel, zbieranie, minimalizacja, użycie/ujawnianie oraz środki kontrolne dotyczące uczestnictwa
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Struktura zapisu zgody i potwierdzenia udzielenia zgody, gdy są stosowane

1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące prywatności dla marketingu, plików cookie, technologii śledzących, analityki, technologii reklamowych (adtech), segmentacji odbiorców, marketingu bezpośredniego, zarządzania preferencjami, blokady kontaktu, tagów stron trzecich, przeglądu kampanii oraz powiązanego przetwarzania PII.

1.2 Niniejsza polityka ma zastosowanie w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania. Obowiązki administratora mają zastosowanie, gdy organizacja określa cele i sposoby marketingu. Obowiązki podmiotu przetwarzającego i podwykonawcy przetwarzania mają zastosowanie wyłącznie wtedy, gdy organizacja przetwarza PII związane z marketingiem, analityką, śledzeniem lub kampaniami na podstawie udokumentowanych poleceń klienta albo nadrzędnego podmiotu przetwarzającego.

1.3 Niniejsza polityka obejmuje:

- 1.3.1 inwentarz przetwarzania marketingowego i powiązanie z celami;
- 1.3.2 dowody zgody i preferencji dotyczące marketingu i śledzenia;
- 1.3.3 nadzór nad plikami cookie, technologiami śledzącymi i tagami;
- 1.3.4 zapisy klauzul informacyjnych dotyczących marketingu i informacji o plikach cookie;
- 1.3.5 kierowanie blokad kontaktu, wycofań zgody i rezygnacji;
- 1.3.6 nadzór nad relacjami z dostawcami marketingowymi, dostawcami analityki i adtech;
- 1.3.7 kierowanie transferów międzynarodowych dotyczących dostawców i platform marketingowych;
- 1.3.8 dowody przeglądu i monitorowania kampanii.

1.4 Niniejsza polityka nie tworzy odrębnego rejestru plików cookie, rejestru tagów, rejestru blokad kontaktu, rejestru kampanii marketingowych, rejestru analityki, procesu obsługi porad prawnych, komitetu, pulpitu, formularza ani niekanonicznej roli.

1.5 Niniejsza polityka nie zastępuje:

- 1.5.1 PII03 w zakresie inwentarza przetwarzania i własności podstawy prawnej;
- 1.5.2 PII04 w zakresie ogólnego nadzoru nad klauzulami informacyjnymi;
- 1.5.3 PII05 w zakresie zarządzania zgodą i preferencjami;
- 1.5.4 PII06 w zakresie procesu obsługi wniosków o realizację praw osób, których dane dotyczą;
- 1.5.5 PII07 w zakresie metodyki oceny ryzyka dla prywatności i DPIA;
- 1.5.6 PII08 w zakresie bramek privacy by design i privacy by default;
- 1.5.7 PII09 w zakresie ogólnych kontroli zbierania, użycia, ujawniania i udostępniania;
- 1.5.8 PII10 w zakresie wykonywania okresów przechowywania, usuwania i utylizacji;
- 1.5.9 PII11 w zakresie nadzoru nad prawidłowością i jakością danych;
- 1.5.10 PII12 w zakresie nadzoru nad cyklem życia podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich;
- 1.5.11 PII13 w zakresie oceny mechanizmu transferów międzynarodowych;
- 1.5.12 PII14 w zakresie architektury bezpieczeństwa PII i kontroli dostępu;
- 1.5.13 PII15 w zakresie obsługi incydentów PII i naruszeń ochrony PII;
- 1.5.14 PII18 w zakresie nadzoru nad monitorowaniem, audytem i doskonaleniem PIMS;
- 1.5.15 PII20 w zakresie zabezpieczeń dotyczących marketingu lub śledzenia specyficznych dla dzieci;
- 1.5.16 PII21 w zakresie kontroli prywatności dotyczących AI, profilowania i zautomatyzowanego podejmowania decyzji;

1.5.17 PII23 w zakresie kontroli podmiotu przetwarzającego PII w chmurze obliczeniowej, gdy ma zastosowanie.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby przetwarzanie związane z marketingiem, plikami cookie, analityką, śledzeniem i adtech było objęte nadzorem poprzez jasne zapisy celów, przejrzyste klauzule informacyjne, odpowiednie kontrole zgody lub preferencji, obsługę blokad kontaktu i wycofań zgody, nadzór nad stronami trzecimi oraz dowody zapewniające gotowość do audytu.

2.2 Niniejsza polityka wspiera rozliczalność w zakresie prywatności w środowiskach B2C, intensywnie korzystających z analityki, wykorzystujących adtech oraz intensywnie zarządzających zgodami, bez wprowadzania niekanonicznych rejestrów, ról ani powielających się procesów.

3. Cele

3.1 Cele niniejszej polityki są następujące:

3.1.1 Zapewnienie, aby cele marketingu i śledzenia były zapisane przed rozpoczęciem przetwarzania.

3.1.2 Zapewnienie, aby dowody zgody, preferencji, blokady kontaktu i wycofania były utrzymywane w kanonicznych obiektach dowodowych.

3.1.3 Zapewnienie, aby informacje o plikach cookie i klauzule informacyjne dotyczące marketingu były aktualne, objęte kontrolą wersji i powiązane z rejestrami przetwarzania.

3.1.4 Zapewnienie, aby technologie śledzące, tagi, piksele, SDKs, narzędzia analityczne i integracje adtech były zatwierdzone przed użyciem produkcyjnym.

3.1.5 Zapewnienie, aby dostawcy marketingowi, dostawcy analityki i partnerzy reklamowi byli klasyfikowani i nadzorowani poprzez kanoniczne dowody relacji.

3.1.6 Zapewnienie spójnego kierowania rezygnacji, sprzeciwów, wycofań zgody i skarg dotyczących marketingu bezpośredniego.

3.1.7 Zapewnienie, aby w stosownych przypadkach wykonywano kierowanie transferów międzynarodowych dotyczących dostawców marketingowych i dostawców analityki.

3.1.8 Zapewnienie, aby kontrole kampanii i śledzenia były monitorowane, przeglądane i doskonalone z wykorzystaniem dowodów PIMS.

4. Postanowienia polityki

4.1 Inwentarz przetwarzania marketingowego i śledzenia

4.1.1 [Controller] Process Owner / Business Owner MUSI zapisać każdą kampanię marketingową, kanał, cel przetwarzania, kategorię PII, źródło odbiorców, powiązanie z podstawą prawną, kategorię technologii śledzącej, zależność od dostawcy lub tagu, powiązanie z klauzulą informacyjną, zależność od zgody lub preferencji, powiązanie z okresem przechowywania oraz flagę transferu w REG02 przed rozpoczęciem kampanii lub działania śledzącego.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUSI potwierdzić, że każdy cel marketingowy w REG02 ma aktualne powiązanie z klauzulą informacyjną REG07 oraz powiązanie ze zgodą lub preferencją REG05 przed uruchomieniem kampanii.

4.1.3 [Processor] Process Owner / Business Owner MUSI udokumentować zatwierdzone przez klienta cele marketingowe oraz polecenia klienta w REG02 lub REG08 przed przetwarzaniem PII marketingowych w imieniu administratora.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MUSI zapisać podział odpowiedzialności współadministratorów w REG08 przed uruchomieniem wspólnego marketingu, kampanii z

wykorzystaniem wspólnej grupy odbiorców, kampanii współbrandowanej lub wspólnego działania śledzącego.

4.1.5 [Conditional] Privacy Lead / PIMS Manager MUSI skierować działania marketingowe obejmujące dostawcę międzynarodowego, tag, dostawcę analityki, platformę reklamową, transfer odbiorców lub transfer polegający na udostępnianiu danych do REG09 przed uruchomieniem produkcyjnym.

4.1.6 [Controller] Process Owner / Business Owner MUSI zapisać wymagania dotyczące blokady kontaktu, wykluczenia lub zakazu kontaktu związane z każdym celem marketingowym w REG05 przed aktywacją.

4.2 Kontrole zgody, preferencji i plików cookie

4.2.1 [Controller] Process Owner / Business Owner MUSI określić, czy dla każdego kanału marketingowego wymagana jest zgoda, preferencja, sprzeciw, polecenie umowne lub inna zatwierdzona podstawa, oraz zapisać decyzję w REG02 i REG05 przed zebraniem danych lub wykorzystaniem ich w kampanii.

4.2.2 [Controller] System Owner / Application Owner MUSI skonfigurować niekonieczne pliki cookie, tagi, piksele, SDKs i podobne technologie śledzące tak, aby pozostawały nieaktywne do czasu dostępności wymaganego stanu zgody lub preferencji w REG05 przed wdrożeniem.

4.2.3 [Controller] System Owner / Application Owner MUSI zwalidować, że sygnały zgody lub preferencji nie są nadpisywane, obchodzone ani ignorowane podczas zmian strony internetowej, aplikacji, kampanii lub menedżera tagów, oraz zapisać dowody walidacji w REG05 lub REG12 przed wydaniem.

4.2.4 [Controller] Process Owner / Business Owner MUSI zapisać dowody zgody, preferencji, wycofania, blokady kontaktu i wersji w REG05 w ciągu jednego dnia roboczego od ich pozyskania, zmiany lub wycofania.

4.2.5 [Processor] System Owner / Application Owner MUSI zastosować dane dotyczące zgody, preferencji, blokady kontaktu lub poleceń przekazane przez klienta do narzędzi marketingowych zarządzanych przez podmiot przetwarzający w terminie uzgodnionym z klientem oraz zapisać zakończenie w REG05 lub REG08.

4.2.6 [Conditional] Privacy Lead / PIMS Manager MUSI utrzymywać mapowanie pól potwierdzenia udzielenia zgody w REG05 przed wydaniem potwierdzeń udzielenia zgody dla celów marketingowych, plików cookie lub śledzenia.

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

9. Wyjątki

9.1 [All] Process Owner / Business Owner MUSI wnioskować o wyjątek w REG12 przed użyciem jakiegokolwiek niestandardowego kanału marketingowego, tagu, konfiguracji analitycznej, mechanizmu preferencji lub dostawcy, gdy wymagane dowody nie mogą zostać skompletowane przed uruchomieniem.

9.2 [Conditional] Data Protection Officer / Privacy Advisor MUSI przejrzeć wnioski o wyjątek dotyczący prywatności w marketingu w REG12 przed zatwierdzeniem, gdy wyjątek wpływa na zgodę, dzieci, pracowników, wrażliwe grupy odbiorców, transfer transgraniczny, profilowanie lub istotne rozszerzenie śledzenia.

9.3 [All] Top Management MUSI zatwierdzić wyjątki dotyczące prywatności w marketingu wysokiego ryzyka lub istotne wyjątki w REG12, zanim wyjątek stanie się skuteczny.

9.4 [All] Privacy Lead / PIMS Manager MUSI ustalić datę wygaśnięcia, właściciela działań naprawczych i datę przeglądu w REG12 dla każdego zatwierzonego wyjątku dotyczącego prywatności w marketingu przed zatwierdzeniem.

10. Egzekwowanie

10.1 [All] Privacy Lead / PIMS Manager MUSI zawiesić lub zablokować działanie marketingowe w REG12, gdy wymagane dowody REG02, REG05, REG07, REG08 lub REG09 są brakujące przed uruchomieniem lub dalszym użyciem.

10.2 [All] System Owner / Application Owner MUSI wyłączyć niezatwierdzone tagi, trackery, piksele, SDKs lub przepływy danych kampanii w ciągu jednego dnia roboczego po decyzji egzekwującej oraz zapisać zakończenie w REG08 lub REG12.

10.3 [All] Vendor / Procurement Owner MUSI zablokować onboarding, odnowienie lub rozszerzenie zakresu dostawcy marketingowego, dostawcy analityki lub platformy reklamowej, gdy wymagane dowody REG08 lub REG09 są brakujące przed rozpoczęciem lub kontynuacją przetwarzania.

10.4 [All] Process Owner / Business Owner MUSI wstrzymać wykorzystanie objętych problemem PII w kampanii w ciągu jednego dnia roboczego po potwierdzonej nieskuteczności kontroli preferencji, blokady kontaktu, klauzuli informacyjnej lub dostawcy oraz zapisać zakończenie w REG05 lub REG12.

10.5 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących dla dużych lub powtarzających się niezgodności dotyczących prywatności w marketingu w REG12 w ciągu 60 dni po zamknięciu działania korygującego.

11. Przegląd i utrzymanie

11.1 [All] Privacy Lead / PIMS Manager MUSI przeglądać niniejszą politykę w REG12 raz w roku oraz w ciągu 30 dni po istotnej zmianie wymagań dotyczących marketingu, plików cookie, śledzenia, analityki, adtech lub zarządzania zgodami.

11.2 [Controller] Process Owner / Business Owner MUSI przeglądać zapisy przetwarzania marketingowego REG02 i zależności preferencji REG05 co najmniej kwartalnie oraz w ciągu 30 dni po istotnej zmianie kampanii.

11.3 [Controller] Privacy Lead / PIMS Manager MUSI przeglądać zapisy klauzul informacyjnych dotyczących marketingu i informacji o plikach cookie w REG07 co najmniej raz w roku oraz w ciągu 30 dni po istotnej zmianie klauzuli informacyjnej, śledzenia lub preferencji.

11.4 [All] Vendor / Procurement Owner MUSI przeglądać zapisy dostawców marketingowych, tagów, analityki i platform reklamowych w REG08 co najmniej raz w roku oraz przed odnowieniem.

11.5 [Conditional] Privacy Lead / PIMS Manager MUSI zaktualizować kierowanie transferów REG09 w ciągu 15 dni roboczych po zidentyfikowanej zmianie dostawcy marketingowego, dostawcy analityki lub lokalizacji hostingu.

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

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 podstawy prawnej

12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.6 PII05 - Polityka zarządzania zgodą i preferencjami

- 12.7 PII06 - Polityka zarządzania prawami osób, których dane dotyczą
- 12.8 PII07 - Polityka oceny ryzyka dla prywatności i DPIA
- 12.9 PII08 - Polityka privacy by design i privacy by default
- 12.10 PII09 - Polityka zbierania, używania, ujawniania i udostępniania PII
- 12.11 PII10 - Polityka retencji, usuwania i utylizacji PII
- 12.12 PII11 - Polityka prawidłowości i jakości PII
- 12.13 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich
- 12.14 PII13 - Polityka międzynarodowych transferów PII
- 12.15 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu
- 12.16 PII15 - Polityka zarządzania incydentami PII i naruszeniami ochrony PII
- 12.17 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS
- 12.18 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS
- 12.19 PII19 - Polityka prywatności pracowników
- 12.20 PII20 - Polityka prywatności dzieci
- 12.21 PII21 - Polityka prywatności dotycząca AI i zautomatyzowanego podejmowania decyzji
- 12.22 PII23 - Polityka podmiotu przetwarzającego PII w chmurze obliczeniowej

13. Normy i ramy odniesienia

- 13.1 Niniejsza polityka została zmapowana 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 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1; 7.2; 7.6; 11.1].
- 13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.4; 6.1; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.1; 4.2.4; 4.2.6; 4.5.1; 4.7.2; 7.1; 11.2].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 5.6; 6.4; 7.5; 11.4].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.10. Addressed by clauses [4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 7.2].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.1.1; 4.2.2; 4.4.4; 4.5.1; 4.5.2; 4.5.4; 4.5.5; 4.7.2; 7.2].
- 13.9 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.1.5; 4.4.3; 4.4.6; 7.5; 11.5].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.3; 4.2.5; 4.3.4; 4.4.5; 7.4].
- 13.11 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.2.5; 4.3.4; 4.4.6; 4.6.3; 7.4; 7.5].
- 13.12 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.2.3; 4.4.4; 4.7.1; 4.7.3; 5.7; 7.2; 10.2].

- 13.13 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.5.1; 4.5.2; 4.7.2; 8.1].
- 13.14 GDPR - Article 6; Article 7. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.2.6; 4.6.2; 7.2].
- 13.15 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.5; 11.3].
- 13.16 GDPR - Article 21. Addressed by clauses [4.5.2; 4.6.1; 4.6.2; 4.6.4; 8.3].
- 13.17 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 4.7.3; 5.6; 5.7; 6.2; 6.4; 8.4; 10.3].
- 13.18 GDPR - Article 44. Addressed by clauses [4.1.5; 4.4.6; 7.5; 11.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.3; 4.6.1; 4.6.2].
- 13.20 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.5.1; 4.5.2; 4.5.4; 4.7.2].
- 13.21 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.1; 4.7.3; 4.7.4; 6.1; 8.5; 10.5].
- 13.22 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.2].
- 13.23 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.2.4; 4.2.6; 7.1; 7.2].