

|                           |          |                                     |          |   |           |  |           |  |         |  |      |
|---------------------------|----------|-------------------------------------|----------|---|-----------|--|-----------|--|---------|--|------|
|                           |          |                                     |          | Wprowadź tutaj nazwę zarejestrowanej osoby prawnej  |           |  |           |  |         |  |      |
| Numer dokumentu:<br>PII21 |          |                                     |          | Tytuł dokumentu:<br><b>Polityka prywatności dotycząca AI i zautomatyzowanego podejmowania decyzji</b> |           |  |           |  |         |  |      |
| 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 |
|                 |            |      |        |
|                 |            |      |        |

|   |
|---|
| <p><b>Nota prawna (prawa autorskie i ograniczenia użytkowania)</b><br/>(C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.<br/>Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.<br/>W sprawach licencjonowania prosimy o kontakt: <a href="mailto:info@clarysec.com">info@clarysec.com</a></p> |
|---|

## Dostosowanie do norm i regulacji

| Norma / regulacja  | Klauzula / środek kontrolny / artykuł                                 | Stosowalność | Typ pokrycia | Komentarz   |
|--------------------|---|--------------|--------------|---|
| ISO/IEC 27701:2025 | Clause 7.5;<br>Clause 8.1   | Both         | Primary      | Udokumentowana informacja i kontrola operacyjna dla dowodów przetwarzania związanego z AI, profilowaniem i zautomatyzowanym podejmowaniem decyzji |
| ISO/IEC 27701:2025 | Clause 9.1;<br>Clause 10.2  | Both         | Supporting   | Monitorowanie, niezgodności i działania korygujące dotyczące środków kontroli prywatności dla AI  |
| ISO/IEC 27701:2025 | Annex A.1.2.2;<br>Annex A.1.2.3;<br>Annex A.1.2.6;<br>Annex A.1.2.9   | Controller   | Primary      | Cel, podstawa prawna, ocena wpływu na prywatność i rejestry administratora  |
| ISO/IEC 27701:2025 | Annex A.1.2.7;<br>Annex A.1.2.8                                       | Controller   | Supporting   | Umowy z podmiotami przetwarzającymi i odpowiedzialności współadministratorów dotyczące przetwarzania PII związanego z AI                          |
| ISO/IEC 27701:2025 | Annex A.1.3.2;<br>Annex A.1.3.3;<br>Annex A.1.3.4                     | Controller   | Primary      | Obowiązki wobec osób, których dane dotyczą, oraz przejrzystość przetwarzania związanego z AI  |
| ISO/IEC 27701:2025 | Annex A.1.3.6;<br>Annex A.1.3.7;<br>Annex A.1.3.10;<br>Annex A.1.3.11 | Controller   | Primary      | Sprzeciw, dostęp, sprostowanie, usunięcie, obsługa wniosków oraz obowiązki dotyczące zautomatyzowanego podejmowania decyzji                       |
| ISO/IEC 27701:2025 | Annex A.1.4.2;<br>Annex A.1.4.3;<br>Annex A.1.4.5                     | Controller   | Primary      | Ograniczenia gromadzenia, przetwarzania i minimalizacji danych wejściowych, wyników   |

|                    |   |             |            |   |
|--------------------|---|-------------|------------|---|
|                    |   |             |            | i danych pochodnych AI  |
| ISO/IEC 27701:2025 | Annex A.1.5.2;<br>Annex A.1.5.3;<br>Annex A.1.5.4;<br>Annex A.1.5.5                                     | Conditional | Supporting | Przekazywanie międzynarodowe, ujawnianie i kierowanie wniosków o ujawnienie dotyczących PII związanego z AI                         |
| ISO/IEC 27701:2025 | Annex A.2.2.2;<br>Annex A.2.2.3;<br>Annex A.2.2.6;<br>Annex A.2.2.7                                     | Processor   | Primary    | Umowa z podmiotem przetwarzającym, udokumentowane polecenia, wsparcie obowiązków klienta i rejestry                                 |
| ISO/IEC 27701:2025 | Annex A.2.3.2;<br>Annex A.2.5.2;<br>Annex A.2.5.3;<br>Annex A.2.5.4;<br>Annex A.2.5.5;<br>Annex A.2.5.6 | Processor   | Supporting | Wsparcie podmiotu przetwarzającego dla obowiązków wobec osób, których dane dotyczą, kierowanie transferów i obsługa ujawnień        |
| ISO/IEC 27701:2025 | Annex A.3.14;<br>Annex A.3.25   | Both        | Supporting | Ochrona rejestrów i rejestrowanie związane z przetwarzaniem PII dotyczącym AI   |
| GDPR               | Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)          | Controller  | Primary    | Profilowanie, rzetelność, przejrzystość, ograniczenie celu, minimalizacja, prawidłowość i rozliczalność                             |
| GDPR               | Article 6; Article 9; Article 10  | Controller  | Primary    | Zgodność z prawem, dane szczególnych kategorii oraz zabezpieczenia dotyczące danych o wyrokach skazujących lub czynach zabronionych |
| GDPR               | Article 12; Article 13; Article 14; Article 15  | Controller  | Primary    | Przejrzyste informacje, dostęp i istotne informacje o zautomatyzowanym podejmowaniu decyzji   |
| GDPR               | Article 16; Article 17; Article 18;   | Controller  | Primary    | Sprostowanie, usunięcie,  |

|                    |  |             |            |   |
|--------------------|--|-------------|------------|---|
|                    | Article 21; Article 22   |             |            | ograniczenie, sprzeciw oraz prawa dotyczące zautomatyzowanego podejmowania decyzji  |
| GDPR               | Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39 | Both        | Supporting | Odpowiedzialność administratora, projektowanie/domślne ustawienia, współadministratorzy, podmioty przetwarzające, rejestry, bezpieczeństwo, DPIA i zadania DPO    |
| GDPR               | Article 44   | Conditional | Referenced | Kierowanie transferów międzynarodowych w przetwarzaniu PII związanym z AI   |
| ISO/IEC 29100:2020 | Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7                                     | Both        | Primary    | Zasady celu, gromadzenia, minimalizacji, wykorzystywania, przechowywania, ujawniania, prawidłowości i jakości   |
| ISO/IEC 29100:2020 | Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12                                  | Both        | Supporting | Przejrzystość, uczestnictwo osoby fizycznej, rozliczalność, bezpieczeństwo informacji i zgodność z wymaganiami prywatności  |
| ISO/IEC 29134:2020 | Clause 5.1; Clause 6.2; Clause 6.3   | Both        | Supporting | Korzyści z PIA, określenie progu i przygotowanie do oceny ryzyka dla prywatności związanego z AI  |
| ISO/IEC 29151:2022 | Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10   | Both        | Supporting | Środki kontrolne dotyczące celu, gromadzenia, minimalizacji, wykorzystywania, przechowywania, ujawniania, prawidłowości i uczestnictwa osoby, której dane dotyczą |



## 1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące prywatności dla działań przetwarzania z użyciem sztucznej inteligencji, profilowania, oceny punktowej, rekomendacji, wspomaganie decyzji i zautomatyzowanego podejmowania decyzji, które wykorzystują, wnioskuje, generują, ujawniają lub w inny sposób przetwarzają PII w zakresie PIMS.

### 1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 systemów, aplikacji, modeli, usług, przepływów pracy, silników decyzyjnych, narzędzi oceny punktowej, systemów rekomendacyjnych, modeli analitycznych i procesów zautomatyzowanego podejmowania decyzji wykorzystujących AI, które przetwarzają PII;

1.2.2 profilowania, segmentacji, klasyfikacji, predykcji, wnioskowania, personalizacji, rankingowania, kwalifikowalności, wykrywania oszustw, punktacji ryzyka, decyzji o dostępie, ocen związanych z zatrudnieniem, profilowania dotyczącego dzieci, personalizacji marketingowej oraz podobnego przetwarzania, w którym występuje PII;

1.2.3 PII związanego z AI wykorzystywanego do trenowania, testowania, walidacji, strojenia, monitorowania, wnioskowania produkcyjnego, przeglądu wyników, pomiaru skuteczności działania, badania incydentów lub wycofania modelu;

1.2.4 kontekstów administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania;

1.2.5 dostawców związanych z AI, podmiotów przetwarzających, podwykonawców przetwarzania, odbiorców w ramach udostępniania danych i ścieżek transferów międzynarodowych, które przetwarzają PII.

1.3 Niniejsza polityka nie tworzy pełnych ram ładu AI, systemu zarządzania AI, inwentarza AI, inwentarza modeli, rejestru ryzyka modeli, rejestru rzetelności, rejestru algorytmów, rejestru incydentów AI, komitetu AI, roli właściciela modelu, roli właściciela systemu AI, procesu uzyskiwania porady prawnej ani odrębnego formularza zatwierdzenia AI.

### 1.4 Niniejsza polityka nie zastępuje:

1.4.1 PII03 w zakresie inwentarza przetwarzania, podstawy prawnej i odpowiedzialności za ROPA;

1.4.2 PII04 w zakresie zarządzania klauzulami informacyjnymi;

1.4.3 PII05 w zakresie zarządzania zgodami i preferencjami;

1.4.4 PII06 w zakresie procesu obsługi praw osób, których dane dotyczą;

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

1.4.6 PII08 w zakresie bramek privacy by design i privacy by default;

1.4.7 PII09 w zakresie kontroli gromadzenia, wykorzystywania, ujawniania i udostępniania danych;

1.4.8 PII10 w zakresie realizacji okresów przechowywania, usuwania i utylizacji;

1.4.9 PII11 w zakresie kontroli prawidłowości i jakości;

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

1.4.11 PII13 w zakresie kontroli transferów międzynarodowych;

1.4.12 PII14 w zakresie bezpieczeństwa i kontroli dostępu;

1.4.13 PII15 w zakresie obsługi incydentów i naruszeń;

1.4.14 PII18 w zakresie monitorowania, audytu i doskonalenia;

1.4.15 PII19 w zakresie prywatności pracowników;

1.4.16 PII20 w zakresie prywatności dzieci;

1.4.17 PII22 w zakresie prywatności marketingowej i plików cookies.

## **2. Cel**

- 2.1 Celem niniejszej polityki jest zapewnienie, aby działania związane z AI, profilowaniem i zautomatyzowanym podejmowaniem decyzji obejmujące PII były identyfikowane, dokumentowane, poddawane ocenie ryzyka, przejrzyste, możliwe do zakwestionowania, monitorowane i kontrolowane przez PIMS, bez tworzenia zdublowanych artefaktów ładu specyficznego dla AI.
- 2.2 Niniejsza polityka zapewnia wykazywanie obowiązków dotyczących prywatności przy przetwarzaniu PII związanym z AI za pomocą REG02, REG04, REG06, REG07, REG08, REG09, REG10 i REG12.

## **3. Cele**

### **3.1 Celami niniejszej polityki są:**

- 3.1.1 identyfikowanie w REG02 przetwarzania obejmującego PII z użyciem AI, profilowania i zautomatyzowanego podejmowania decyzji;
- 3.1.2 dokumentowanie w REG02 celów związanych z AI, podstawy prawnej, kategorii PII, źródeł danych, danych wywnioskowanych, wyników, odbiorców i skutków decyzji;
- 3.1.3 uruchamianie wstępnej oceny ryzyka dla prywatności i kierowania do DPIA za pośrednictwem REG04;
- 3.1.4 zapewnienie, aby klauzule informacyjne dotyczące AI i istotne informacje były rejestrowane w REG07;
- 3.1.5 kierowanie wniosków dotyczących praw, sprzeciwu, interwencji ludzkiej i możliwości zakwestionowania za pośrednictwem REG06;
- 3.1.6 kontrolowanie podmiotów przetwarzających, podwykonawców przetwarzania, dostawców i uzgodnień dotyczących udostępniania danych związanych z AI za pośrednictwem REG08;
- 3.1.7 kierowanie transferów międzynarodowych związanych z AI za pośrednictwem REG09;
- 3.1.8 eskalowanie podejrzewanych incydentów PII związanych z AI, niewłaściwego użycia, nieuprawnionego ujawnienia i niekorzystnych skutków dla prywatności za pośrednictwem REG10 i REG12;
- 3.1.9 rejestrowanie monitorowania, wyjątków, niezgodności, działań korygujących i usprawnień w REG12.

## **4. Postanowienia polityki**

### **4.1 Identyfikacja AI, profilowania i zautomatyzowanego podejmowania decyzji**

- 4.1.1 [Controller] Gdy proponowany jest nowy lub istotnie zmieniony system, aplikacja, model, przepływ pracy, usługa lub proces biznesowy, Process Owner / Business Owner musi ustalić, czy wykorzystuje on AI, profilowanie, ocenę punktową, rekomendację, wspomaganie decyzji lub zautomatyzowane podejmowanie decyzji obejmujące PII, oraz odnotować to ustalenie w REG02.
- 4.1.2 [Controller] Przed rozpoczęciem przetwarzania PII związanego z AI Process Owner / Business Owner musi udokumentować w REG02 cel przetwarzania, kategorie PII, kategorie osób, których dane dotyczą, źródła danych, kategorie danych wywnioskowanych lub danych pochodnych, kategorie wyników, kategorie odbiorców, podstawę prawną i powiązanie z okresem przechowywania.
- 4.1.3 [Controller] Przed wykorzystaniem profilowania, oceny punktowej, rekomendacji, wspomaganie decyzji lub zautomatyzowanego podejmowania decyzji w środowisku produkcyjnym Process Owner / Business Owner musi udokumentować kontekst decyzji,

oczekiwany wpływ na osoby, których dane dotyczą, udział człowieka oraz ścieżkę realizacji praw w REG02 i REG04.

- 4.1.4 [Joint Controller] Przed przetwarzaniem PII związanego z AI wraz ze współadministratorem Privacy Lead / PIMS Manager musi udokumentować w REG08 odpowiedzialność za określenie celu, klauzulę informacyjną, obsługę praw, wsparcie DPIA, zarządzanie podmiotem przetwarzającym i eskalację incydentów.
- 4.1.5 [Processor] Przed przetwarzaniem PII za pośrednictwem usługi związanej z AI dla klienta Process Owner / Business Owner musi potwierdzić, że polecenia klienta, dozwolone cele, zakazane zastosowania, postępowanie z wynikami i obowiązki wsparcia są udokumentowane w REG08.
- 4.1.6 [Both] Przed aktywowaniem przetwarzania PII związanego z AI Privacy Lead / PIMS Manager musi potwierdzić, że przetwarzanie jest powiązane z właściwymi kanonicznymi obiektami dowodowymi oraz że poza REG02, REG04, REG06, REG07, REG08, REG09, REG10 lub REG12 nie utworzono odrębnego rejestru specyficznego dla AI.

## **4.2 Ocena ryzyka dla prywatności i kierowanie do DPIA**

- 4.2.1 [Controller] Przed uruchomieniem lub istotną zmianą przetwarzania PII związanego z AI Privacy Lead / PIMS Manager musi przeprowadzić wstępną ocenę ryzyka dla prywatności i odnotować decyzję dotyczącą DPIA w REG04.
- 4.2.2 [Conditional] Gdy przetwarzanie związane z AI obejmuje profilowanie, zautomatyzowane decyzje, ocenę na dużą skalę, dane szczególnych kategorii, dane dotyczące czynów zabronionych, osoby, których dane dotyczą, znajdujące się w sytuacji podatności, ocenę pracowników, dzieci, monitorowanie zachowania, dane lokalizacyjne, dane biometryczne, punktację o istotnym wpływie lub istotne skutki, Data Protection Officer / Privacy Advisor musi przejrzeć ryzyko dla prywatności i odnotować poradę w REG04.
- 4.2.3 [Controller] Przed uruchomieniem produkcyjnym przetwarzania PII związanego z AI Process Owner / Business Owner musi udokumentować działania w zakresie postępowania z ryzykiem, status ryzyka rezydualnego oraz dowody gotowości do uruchomienia produkcyjnego w REG04 lub REG12.
- 4.2.4 [Controller] Przed ponownym wykorzystaniem PII do trenowania, testowania, walidacji, strojenia, monitorowania lub doskonalenia modelu w nowym lub istotnie zmienionym celu Process Owner / Business Owner musi przeprowadzić przegląd prywatności i odnotować decyzję w REG02 i REG04.
- 4.2.5 [Conditional] Gdy ryzyko rezydualne dla prywatności pozostaje wysokie po planowanym postępowaniu z ryzykiem, Top Management musi zatwierdzić, odrzucić lub wymagać dalszego postępowania z ryzykiem przed użyciem produkcyjnym oraz odnotować decyzję w REG04 i REG12.

[ ... 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] Przed odejściem od wymagania dotyczącego prywatności związanej z AI określonego w niniejszej polityce wnioskujący Process Owner / Business Owner musi złożyć uzasadnienie wyjątku oraz dowody kontroli kompensujących w REG12.
- 9.2 [Conditional] Gdy wyjątek wpływa na profilowanie, zautomatyzowane podejmowanie decyzji, interwencję ludzką, możliwość zakwestionowania, przejrzystość, wynik DPIA, punktację o istotnym wpływie, przetwarzanie dotyczące dzieci, przetwarzanie dotyczące pracowników, ograniczenia podmiotu przetwarzającego lub transfery międzynarodowe, Data Protection Officer / Privacy Advisor musi przejrzeć wyjątek i odnotować poradę w REG04 lub REG12.

- 9.3 [Conditional] Gdy wyjątek tworzy lub utrzymuje wysokie ryzyko rezydualne dla prywatności, Top Management musi zatwierdzić albo odrzucić wyjątek oraz odnotować decyzję w REG04 i REG12.
- 9.4 [All] Przed wygaśnięciem zatwierdzonego wyjątku dotyczącego prywatności związanej z AI Privacy Lead / PIMS Manager musi przejrzeć status zamknięcia, odnowienia lub działania korygującego oraz odnotować wynik w REG12.

## 10. Egzekwowanie postanowień

- 10.1 [All] Gdy zostanie zidentyfikowana niezgodność z niniejszą polityką, Privacy Lead / PIMS Manager musi odnotować niezgodność i działanie korygujące w REG12.
- 10.2 [Both] Gdy podejrzewa się nieuprawnione przetwarzanie PII związane z AI, ujawnienie, dostęp, niewłaściwe użycie modelu, nieskuteczność realizacji praw lub niekorzystny skutek dla prywatności, Incident Response Coordinator musi zainicjować eskalację incydentu i odnotować dowody w REG10 i REG12.
- 10.3 [Both] Gdy podmiot przetwarzający, podwykonawca przetwarzania, dostawca lub odbiorca w ramach udostępniania danych nie spełnia obowiązków dotyczących prywatności związanych z AI, Vendor / Procurement Owner musi odnotować działanie naprawcze, eskalacyjne lub wypowiedzenie w REG08 i REG12.
- 10.4 [All] Gdy występują powtarzające się lub systemowe niezgodności dotyczące prywatności związanej z AI, Top Management musi przejrzeć sprawę i odnotować działanie zarządcze w REG12.

## 11. Przegląd i utrzymanie

- 11.1 [All] Co najmniej raz w roku Privacy Lead / PIMS Manager musi przejrzeć niniejszą politykę pod kątem dalszej odpowiedniości i odnotować wynik przeglądu w REG12.
- 11.2 [Conditional] Gdy przepisy prawa, usługi, modele, źródła danych, praktyki profilowania, logika zautomatyzowanego podejmowania decyzji, uzgodnienia z dostawcami, ścieżki transferów lub ryzyka dla prywatności istotnie się zmieniają, Privacy Lead / PIMS Manager musi przejrzeć dotknięte zmianą kontrole prywatności związane z AI i odnotować wynik w REG02, REG04 lub REG12.
- 11.3 [Controller] Co najmniej raz w roku oraz po istotnych zmianach ścieżki użytkownika związanych z AI Process Owner / Business Owner musi przejrzeć dowody dotyczące przejrzystości, istotnych informacji, interwencji ludzkiej i ścieżki realizacji praw oraz odnotować przegląd w REG06 i REG07.
- 11.4 [All] Po zamknięciu działań korygujących dotyczących prywatności związanej z AI Internal Audit / Compliance Reviewer musi zweryfikować skuteczność i odnotować dowody weryfikacji w REG12.

## 12. Powiązane polityki

- 12.1 PII01 - Polityka systemu zarządzania informacjami o prywatności
- 12.2 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności
- 12.3 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej
- 12.4 PII04 - Polityka klauzul informacyjnych i przejrzystości
- 12.5 PII05 - Polityka zarządzania zgodami i preferencjami
- 12.6 PII06 - Polityka zarządzania prawami osób, których dane dotyczą
- 12.7 PII07 - Polityka oceny ryzyka dla prywatności i DPIA
- 12.8 PII08 - Polityka privacy by design i privacy by default
- 12.9 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII
- 12.10 PII10 - Polityka przechowywania, usuwania i utylizacji PII

- 12.11 PII11 - Polityka prawidłowości 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 PII
- 12.16 PII17 - Polityka zarządzania udokumentowaną informacją i dowodami PIMS
- 12.17 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS
- 12.18 PII19 - Polityka prywatności pracowników
- 12.19 PII20 - Polityka prywatności dzieci
- 12.20 PII22 - Polityka prywatności marketingowej i plików cookies

### **13. Normy i ramy odniesienia**

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].
- 13.8 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 [4.7.3; 4.7.4; 4.7.5; 7.7].
- 13.9 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 [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].
- 13.10 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 [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].
- 13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].
- 13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].
- 13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7.  
Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12.  
Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1;  
4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10.  
Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].