

				Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII20				Tytuł dokumentu: Polityka prywatności dzieci							
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

<p>Nota prawna (prawa autorskie i ograniczenia użytkowania) (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. Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych. W sprawach licencjonowania prosimy o kontakt: info@clarysec.com</p>
--

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	Udokumentowana informacja i kontrola operacyjna dotyczące dowodów przetwarzania związanego z dziećmi
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, niezgodność i działania korygujące dotyczące środków kontroli prywatności dzieci
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.1.2.6; Annex A.1.2.9	Controller	Primary	Cele, podstawa prawna, zgoda, DPIA i rejestry administratora dotyczące przetwarzania związanego z dziećmi
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Umowy z podmiotami przetwarzającymi i obowiązki współadministratorów dotyczące przetwarzania związanego z dziećmi
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	Obowiązki wobec dzieci, przekazywanie informacji oraz zmiana lub wycofanie zgody
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Sprzeciw, dostęp, sprostowanie, usunięcie, obsługa wniosków i obowiązki dotyczące zautomatyzowanego podejmowania decyzji
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3;	Controller	Primary	Ograniczenia gromadzenia,

	Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9			przetwarzania, minimalizacji, retencji i utylizacji
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Supporting	Rejestry ujawnień i obsługa wniosków o ujawnienie
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	Primary	Umowa z klientem podmiotu przetwarzającego, polecenia, wsparcie i rejestry
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Wsparcie podmiotu przetwarzającego w zakresie obowiązków wobec osób, których dane dotyczą, oraz obsługi ujawnień
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrona rejestrów i rejestrowanie dowodów przetwarzania związanego z dziećmi
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Rzetelność, przejrzystość, ograniczenie celu, minimalizacja, ograniczenie przechowywania i rozliczalność
GDPR	Article 6; Article 7; Article 8; Article 9	Controller	Primary	Zgodność z prawem, warunki zgody, zgoda dziecka i zabezpieczenia dotyczące szczególnych kategorii danych
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Przejrzyste informacje i klauzule informacyjne dostosowane do dzieci
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Prawa dostępu, sprostowania, usunięcia, ograniczenia, sprzeciwu i 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, ochrona danych w fazie projektowania i domyślna ochrona danych, współadministratorzy, podmioty przetwarzające, rejestry, bezpieczeństwo, DPIA i zadania DPO
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Zgoda i wybór, przejrzystość oraz udział osoby fizycznej
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Ograniczenie celu, gromadzenia, minimalizacji, wykorzystywania, retencji i ujawniania
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Rozliczalność, bezpieczeństwo informacji i zgodność w zakresie prywatności
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Korzyści z PIA, ustalenie progu i przygotowanie do oceny ryzyka związanego z dziećmi
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Zgoda, cel, gromadzenie, minimalizacja, retencja, ujawnianie i środki kontrolne dotyczące udziału osoby, której dane dotyczą
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 stosowane są potwierdzenia udzielenia zgody

1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące prywatności dla przetwarzania PII obejmującego dzieci, usług skierowanych do dzieci, usług, do których dzieci prawdopodobnie uzyskają dostęp, oraz czynności przetwarzania, w których PII dzieci wymagają wzmocnionych zabezpieczeń.

1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 czynności przetwarzania PII obejmujących dzieci w zakresie PIMS;

1.2.2 stron internetowych, aplikacji, gier, usług edukacyjnych, platform internetowych, usług połączonych, portali klienta, środowisk nauczania, społeczności i kanałów wsparcia skierowanych do dzieci;

1.2.3 przetwarzania, w którym dzieci są bezpośrednimi adresatami, prawdopodobnymi użytkownikami, posiadaczami kont, uczniami, uczestnikami, beneficjentami lub reprezentowanymi osobami, których dane dotyczą;

1.2.4 oceny wieku, odpowiedzialności rodzicielskiej lub zgody albo aprobaty osoby sprawującej władzę rodzicielską, klauzul informacyjnych przyjaznych dziecku, dowodów zgody, oceny ryzyka dla prywatności, przesłanek DPIA, minimalizacji, obsługi praw, ograniczeń dotyczących podmiotów przetwarzających, udostępniania danych i eskalacji związanej z bezpieczeństwem obejmującej PII dzieci;

1.2.5 kontekstów administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania.

1.3 Niniejsza polityka nie zastępuje:

1.3.1 PII03 w zakresie inwentarza przetwarzania, podstawy prawnej i własności ROPA;

1.3.2 PII04 w zakresie ogólnego nadzoru nad klauzulami informacyjnymi;

1.3.3 PII05 w zakresie działania zarządzania zgodą i preferencjami;

1.3.4 PII06 w zakresie procesu obsługi wniosków osób, których dane dotyczą, o realizację praw;

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

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

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

1.3.8 PII10 w zakresie wykonywania retencji, usuwania i utylizacji;

1.3.9 PII11 w zakresie kontroli prawidłowości i jakości;

1.3.10 PII12 w zakresie nadzoru nad cyklem życia podmiotu przetwarzającego, podwykonawcy przetwarzania i strony trzeciej;

1.3.11 PII13 w zakresie kontroli międzynarodowych transferów;

1.3.12 PII14 w zakresie bezpieczeństwa i kontroli dostępu;

1.3.13 PII15 w zakresie obsługi incydentów i naruszeń;

1.3.14 PII18 w zakresie monitorowania, audytu i doskonalenia;

1.3.15 PII21 w zakresie kontroli prywatności dotyczących AI i zautomatyzowanego podejmowania decyzji;

1.3.16 PII22 w zakresie kontroli prywatności w marketingu i plików cookie.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby PII dzieci były identyfikowane, objęte nadzorem, minimalizowane, wyjaśniane, chronione i dokumentowane za pomocą wzmocnionych zabezpieczeń prywatności odpowiednich dla przetwarzania skierowanego do dzieci i dostępnego dla dzieci.

2.2 Niniejsza polityka wspiera spójne podejmowanie decyzji dotyczących przetwarzania związanego z dziećmi bez tworzenia odrębnego rejestru danych dzieci, rejestru zapewnienia wieku, rejestru zgód lub aprobat osób sprawujących władzę rodzicielską, pulpitu bezpieczeństwa, komitetu ani niekanonicznego obiektu dowodowego.

3. Cele szczegółowe

3.1 Celami niniejszej polityki są:

- 3.1.1 identyfikowanie czynności przetwarzania skierowanych do dzieci i dostępnych dla dzieci w REG02;
- 3.1.2 określenie oczekiwań dotyczących oceny wieku oraz zgody albo aprobaty osoby sprawującej władzę rodzicielską bez wskazywania w polityce progów wieku właściwych dla poszczególnych jurysdykcji;
- 3.1.3 zapewnienie utrzymywania klauzul informacyjnych przyjaznych dziecku w REG07;
- 3.1.4 zapewnienie utrzymywania dowodów zgody, zgody albo aprobaty osoby sprawującej władzę rodzicielską i wycofania zgody w REG05, gdy ma to zastosowanie;
- 3.1.5 uruchamianie oceny ryzyka dla prywatności właściwej dla dzieci i ścieżki DPIA przez REG04;
- 3.1.6 zapewnienie, aby wnioski o realizację praw dotyczące dzieci były obsługiwane przez REG06;
- 3.1.7 ograniczanie podmiotów przetwarzających, podwykonawców przetwarzania i udostępniania danych obejmującego PII dzieci przez REG08;
- 3.1.8 kierowanie podejrzewanych incydentów PII dzieci, niewłaściwego użycia, nieuprawnionego dostępu lub ryzyk dotyczących PII związanych z bezpieczeństwem przez REG10 i REG12;
- 3.1.9 utrzymywanie dowodów gotowych do audytu dla nadzoru nad prywatnością dzieci przez REG12.

4. Postanowienia polityki

4.1 Identyfikacja i autoryzacja przetwarzania skierowanego do dzieci

- 4.1.1 [Controller] Gdy proponowana jest nowa lub istotnie zmieniona usługa, funkcja, kampania, kanał lub czynność przetwarzania, Process Owner / Business Owner musi ustalić, czy przetwarzanie jest skierowane do dzieci, czy prawdopodobnie będzie dostępne dla dzieci lub czy w inny sposób obejmuje PII dzieci, oraz odnotować ustalenie w REG02.
- 4.1.2 [Controller] Przed gromadzeniem informacji związanych z wiekiem Process Owner / Business Owner musi określić minimalne dane do oceny wieku niezbędne do celu przetwarzania oraz odnotować metodę w REG02.
- 4.1.3 [Controller] Przed rozpoczęciem przetwarzania PII dzieci Process Owner / Business Owner musi udokumentować cel przetwarzania, podstawę prawną, skonfigurowany próg wieku dziecka, zależność od zgody albo aprobaty osoby sprawującej władzę rodzicielską oraz lokalizację dowodów w REG02 i REG05, gdy stosowana jest zgoda lub aprobata.
- 4.1.4 [Joint Controller] Przed przetwarzaniem PII dzieci ze współadministratorem Privacy Lead / PIMS Manager musi udokumentować obowiązki dotyczące prywatności dzieci, odpowiedzialność za klauzulę informacyjną, obsługę praw, odpowiedzialność za zgodę lub aprobatę oraz odpowiedzialność za eskalację w REG08.
- 4.1.5 [Processor] Przed przetwarzaniem PII dzieci dla klienta Process Owner / Business Owner musi potwierdzić, że polecenia dotyczące przetwarzania związanego z dziećmi są udokumentowane i odzwierciedlone w REG08.

- 4.1.6 [Both] Przed aktywowaniem przetwarzania PII dzieci w systemie lub procesie biznesowym Privacy Lead / PIMS Manager musi potwierdzić, że znaczniki danych dzieci, odpowiedzialni właściciele i wymagane obiekty dowodowe zostały odnotowane w REG02 albo REG08, zależnie od zastosowania.

4.2 Przejrzystość i klauzule informacyjne przyjazne dziecku

- 4.2.1 [Controller] Przed gromadzeniem PII dzieci bezpośrednio od dziecka lub rodzica Process Owner / Business Owner musi zapewnić dostępność klauzuli informacyjnej odpowiedniej dla dziecka oraz jej odnotowanie w REG07.
- 4.2.2 [Controller] Gdy usługa jest zaprojektowana dla dzieci lub prawdopodobnie będzie dostępna dla dzieci, Process Owner / Business Owner musi zapewnić warstwową treść klauzuli informacyjnej, która oddziela wyjaśnienia odpowiednie dla dziecka od informacji dla rodzica lub opiekuna, oraz odnotować wersję klauzuli w REG07.
- 4.2.3 [Controller] Gdy PII dzieci są gromadzone pośrednio, Process Owner / Business Owner musi udokumentować źródło, podejście do klauzuli informacyjnej oraz termin przekazania klauzuli w REG02 i REG07.
- 4.2.4 [Controller] Gdy zmienia się cel przetwarzania skierowanego do dzieci, kategoria danych, kategoria odbiorcy, odniesienie do retencji, mechanizm uzyskiwania zgody lub ścieżka realizacji praw, Privacy Lead / PIMS Manager musi przejrzeć i zaktualizować odpowiedni zapis klauzuli informacyjnej w REG07 przed wdrożeniem zmiany.

[... 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 odstępniem od wymagania dotyczącego prywatności dzieci określonego w niniejszej polityce wnioskujący Process Owner / Business Owner musi przedstawić w REG12 uzasadnienie wyjątku i dowody środka kompensującego.
- 9.2 [Conditional] Gdy wyjątek wpływa na zgodę dziecka, zgodę albo aprobatę osoby sprawującej władzę rodzicielską, klauzulę informacyjną skierowaną do dzieci, profilowanie, zautomatyzowane podejmowanie decyzji, wynik DPIA, ujawnianie lub przetwarzanie związane z bezpieczeństwem, Data Protection Officer / Privacy Advisor musi przejrzeć wyjątek i odnotować poradę w REG04 albo REG12.
- 9.3 [Conditional] Gdy wyjątek tworzy lub utrzymuje wysokie ryzyko rezydualne dla PII dzieci, Top Management musi zatwierdzić albo odrzucić wyjątek i odnotować decyzję w REG04 i REG12.
- 9.4 [All] Przed wygaśnięciem zatwierdzonego wyjątku dotyczącego prywatności dzieci Privacy Lead / PIMS Manager musi przejrzeć status zamknięcia, odnowienia lub działania korygującego i 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 podejrzewane jest nieuprawnione przetwarzanie, ujawnienie, dostęp lub wykorzystanie PII dzieci, 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 udostępniania danych nie spełnia obowiązków dotyczących prywatności dzieci, Vendor / Procurement Owner musi odnotować działanie naprawcze, eskalacyjne lub rozwiązujące współpracę w REG08 i REG12.

- 10.4 [All] Gdy występują powtarzające się lub systemowe niezgodności dotyczące prywatności dzieci, 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 dokonać przeglądu niniejszej polityki pod kątem dalszej odpowiedniości i odnotować wynik przeglądu w REG12.
- 11.2 [Conditional] Gdy przepisy prawa, usługi, technologie, metody oceny wieku, mechanizmy uzyskiwania zgody, ścieżki użytkownika skierowane do dzieci lub ryzyka przetwarzania ulegają istotnej zmianie, Privacy Lead / PIMS Manager musi przejrzeć dotknięte kontrole prywatności dzieci i odnotować wynik w REG02, REG04 albo REG12.
- 11.3 [Controller] Co najmniej raz w roku oraz po istotnych zmianach interfejsu Process Owner / Business Owner musi przejrzeć treść klauzul informacyjnych i zgód skierowanych do dzieci oraz odnotować przegląd w REG05 i REG07.
- 11.4 [All] Po zamknięciu działań korygujących dotyczących prywatności dzieci 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 zgodą 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 retencji, 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 międzynarodowych transferów PII
- 12.14 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu
- 12.15 PII15 - Polityka zarządzania incydentami PII i naruszeniami
- 12.16 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS
- 12.17 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS
- 12.18 PII21 - Polityka prywatności dotycząca AI i zautomatyzowanego podejmowania decyzji
- 12.19 PII22 - Polityka prywatności w marketingu i plików cookie

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 [4.8.2; 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.1.2.4; Annex A.1.2.5; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.3.1; 4.3.2; 4.3.5; 4.6.1; 4.8.1; 7.1; 7.2; 7.4].

- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].
- 13.5 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 [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.3; 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 [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.3; 4.6.5; 7.6].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 7.1].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.1; 4.7.2; 4.8.1; 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; 4.5.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2). Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.4; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 7; Article 8; Article 9. Addressed by clauses [4.1.3; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.4.3; 7.4; 11.3].
- 13.14 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.3; 11.3].
- 13.15 GDPR - Article 15; 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; 4.6.3; 4.6.5; 7.6].
- 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; 4.6.1; 4.6.2; 4.7.3; 4.8.2; 5.3; 6.4; 7.2; 9.2].
- 13.17 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.3.1; 4.3.3; 4.5.1; 4.5.2; 4.5.3].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 4.4.4; 4.4.5; 4.7.1].
- 13.19 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 4.8.2; 6.1; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.4.3; 4.6.1; 4.6.3; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 4.5.2; 4.7.1; 7.4].
- 13.22 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.3.2; 4.3.4; 4.3.5; 7.4].