

				Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: PII21				Dokumento pavadinimas: <b>DI ir automatizuoto sprendimų priėmimo privatumo politika</b>							
Versija: 1.0		Įsigaliojimo data: 01.01.2025		Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita

Peržiūrų istorija				
Peržiūros numeris	Peržiūros data	Pakeitimai	Peržiūrėjo	Proceso savininkas

Patvirtinimai			
Vardas	Pareigos	Data	Parašas

**Teisinis pranešimas (autorių teisės ir naudojimo apribojimai)**  
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokumentas yra Clarysec LLC intelektinė nuosavybė. Jokia šio dokumento dalis negali būti kopijuojama, pakartotinai naudojama, platinama ar keičiama komerciniais ar įgyvendinimo tikslais be išankstinio aiškaus rašytinio leidimo.

Neautorizuotas naudojimas yra griežtai draudžiamas ir gali užtraukti teisinius veiksmus.

Dėl licencijavimo kreipkitės: [info@clarysec.com](mailto:info@clarysec.com)

## Suderinta su standartais ir reglamentais

Standartas / reglamentas	Nuostata / kontrolė / straipsnis	Taikymas	Aprėpties tipas	Komentaras
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentuota informacija ir operacinė kontrolė, skirta DI, profiliavimo ir automatizuoto sprendimų priėmimo tvarkymo įrodymams
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	DI privatumo kontrolės priemonių stebėseną, neatitiktys ir korekciniai veiksmai
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Tikslas, teisinis pagrindas, poveikio privatumui vertinimas ir duomenų valdytojo įrašai
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Duomenų tvarkytojų sutartys ir bendrų duomenų valdytojų atsakomybės dėl su DI susijusio PII tvarkymo
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Pareigos duomenų subjektams ir skaidrumas dėl su DI susijusio tvarkymo
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	Prieštaravimo, priegos, taisymo, ištrynimo teisės, prašymų nagrinėjimas ir automatizuoto sprendimų priėmimo pareigos
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	DI įvesčių, išvesčių ir išvestinių duomenų rinkimo,

				tvarkymo ir minimizavimo ribos
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	Su DI susijusio PII tarptautinio perdavimo, atskleidimo ir prašymų atskleisti duomenis nukreipimas
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	Duomenų tvarkytojo susitarimas, dokumentuoti nurodymai, pagalba vykdam kliento pareigas ir įrašai
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	Duomenų tvarkytojo pagalba vykdam pareigas duomenų subjektams, perdavimo nukreipimas ir atskleidimo tvarkymas
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Įrašų apsauga ir žurnalų vedimas, susiję su su DI susijusiu PII tvarkymu
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	Profilavimas, sąžiningumas, skaidrumas, tikslo ribojimas, minimizavimas, tikslumas ir atskaitomybė
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Teisėtumas, specialių kategorijų duomenys ir apkaltinamųjų nuosprendžių ar nusikalstamų veikų duomenų apsaugos priemonės

GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Skaidri informacija, prieiga ir prasminga informacija apie automatizuotą sprendimų priėmimą
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Taisymo, ištyrimo, apribojimo, prieštaravimo ir automatizuoto sprendimų priėmimo teisės
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Duomenų valdytojo atsakomybė, projektavimo ir numatytųjų nustatymų principai, bendri duomenų valdytojai, duomenų tvarkytojai, įrašai, saugumas, DPIA ir DAP užduotys
GDPR	Article 44	Conditional	Referenced	Su DI susijusio PII tvarkymo tarptautinio perdavimo nukreipimas
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Tikslo, rinkimo, minimizavimo, naudojimo, saugojimo, atskleidimo, tikslumo ir kokybės principai
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Skaidrumas, asmens dalyvavimas, atskaitomybė, informacijos saugumas ir privatumo atitiktis
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA nauda, ribos nustatymas ir pasirengimas su DI susijusiam privatumo rizikos vertinimui

ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Tikslo, rinkimo, minimizavimo, naudojimo, saugojimo, atskleidimo, tikslumo ir duomenų subjekto dalyvavimo kontrolės priemonės
-----------------------	---	------	------------	--

## 1. Taikymo sritis

1.1 Ši politika nustato privalomus privatumo reikalavimus dirbtinio intelekto, profiliavimo, vertinimo balais, rekomendavimo, sprendimų priėmimo paramos ir automatizuoto sprendimų priėmimo tvarkymo veikloms, kai jos naudoja, numano, generuoja, atskleidžia ar kitaip tvarko PII PIMS taikymo srityje.

### 1.2 Ši politika taikoma toliau nurodytiems objektams:

1.2.1 DI įgalintoms sistemoms, taikomosioms programoms, modeliams, paslaugoms, darbo eigoms, sprendimų varikliams, vertinimo balais priemonėms, rekomendavimo sistemoms, analitiniams modeliams ir automatizuoto sprendimų priėmimo procesams, kurie tvarko PII;

1.2.2 profiliavimui, segmentavimui, klasifikavimui, prognozavimui, išvedimui, personalizavimui, reitingavimui, tinkamumo vertinimui, sukčiavimo aptikimui, rizikos vertinimui balais, prieigos sprendimams, su darbu susijusiam vertinimui, su vaikais susijusiam profiliavimui, rinkodaros personalizavimui ir panašiam tvarkymui, kai naudojama PII;

1.2.3 su DI susijusiai PII, naudojamai mokymui, testavimui, validavimui, derinimui, stebėsenai, produkciniam išvedimui, išvesties peržiūrai, veikimo matavimui, incidento tyrimui ar modelio eksploatacijos nutraukimui;

1.2.4 duomenų valdytojo, bendro duomenų valdytojo, duomenų tvarkytojo ir subtvarkytojo kontekstams;

1.2.5 su DI susijusiems tiekėjams, duomenų tvarkytojams, subtvarkytojams, duomenų dalijimosi gavėjams ir tarptautinio perdavimo keliams, kurie tvarko PII.

1.3 Ši politika nesukuria visos DI valdysenos sistemos, DI valdymo sistemos, DI apskaitos, modelių apskaitos, modelių rizikos registro, sąžiningumo registro, algoritmų registro, DI incidentų registro, DI komiteto, modelio savininko vaidmens, DI sistemos savininko vaidmens, teisinės konsultacijos darbo eigos ar atskiros DI patvirtinimo formos.

### 1.4 Ši politika nepakeičia toliau nurodytų politikų:

1.4.1 PII03 dėl tvarkymo veiklos apskaitos, teisinio pagrindo ir ROPA savininkystės;

1.4.2 PII04 dėl privatumo pranešimų valdysenos;

1.4.3 PII05 dėl sutikimų ir nuostatų valdymo;

1.4.4 PII06 dėl duomenų subjekto teisių darbo eigos;

1.4.5 PII07 dėl privatumo rizikos vertinimo ir DPIA metodikos;

1.4.6 PII08 dėl privatumo pagal projektavimą ir pagal numatytuosius nustatymus vartų;

1.4.7 PII09 dėl rinkimo, naudojimo, atskleidimo ir dalijimosi kontrolės priemonių;

1.4.8 PII10 dėl saugojimo, ištrynimo ir sunaikinimo vykdymo;

1.4.9 PII11 dėl tikslumo ir kokybės kontrolės priemonių;

1.4.10 PII12 dėl duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių gyvavimo ciklo valdysenos;

1.4.11 PII13 dėl tarptautinio perdavimo kontrolės priemonių;

1.4.12 PII14 dėl saugumo ir prieigos kontrolės;

1.4.13 PII15 dėl incidentų ir pažeidimų valdymo;

1.4.14 PII18 dėl stebėsenos, audito ir tobulinimo;

1.4.15 PII19 dėl darbuotojų privatumo;

1.4.16 PII20 dėl vaikų privatumo;

1.4.17 PII22 dėl rinkodaros privatumo ir slapukų.

## 2. Tikslas

- 2.1 Šios politikos tikslas – užtikrinti, kad su PII susijusios DI, profiliavimo ir automatizuoto sprendimų priėmimo veiklos būtų identifiкуotos, dokumentuotos, įvertintos pagal riziką, skaidrios, su galimybe užginčyti sprendimą, stebimos ir kontroliuojamos per PIMS, nekuriant dubliuojančių DI skirtų valdysenos artefaktų.
- 2.2 Ši politika užtikrina, kad su DI susijusio PII tvarkymo privatumo pareigos būtų pagrindžiamos per REG02, REG04, REG06, REG07, REG08, REG09, REG10 ir REG12.

### 3. Tikslai

#### 3.1 Šios politikos tikslai yra:

- 3.1.1 identifiкуoti DI, profiliavimo ir automatizuoto sprendimų priėmimo tvarkymą, susijusį su PII, REG02;
- 3.1.2 dokumentuoti su DI susijusius tikslus, teisinį pagrindą, PII kategorijas, duomenų šaltinius, numanomas duomenis, išvestis, gavėjus ir sprendimų poveikį REG02;
- 3.1.3 inicijuoti pirminį privatumo rizikos vertinimą ir DPIA nukreipimą per REG04;
- 3.1.4 užtikrinti, kad su DI susiję privatumo pranešimai ir prasminga informacija būtų įrašomi REG07;
- 3.1.5 nukreipti teisių, prieštaravimo, žmogaus atliekamos peržiūros ir sprendimo užginčijimo prašymus per REG06;
- 3.1.6 valdyti su DI susijusius duomenų tvarkytojus, subtvarkytojus, tiekėjus ir duomenų dalijimosi susitarimus per REG08;
- 3.1.7 nukreipti su DI susijusius tarptautinius perdavimus per REG09;
- 3.1.8 eskaluoti įtariamus su DI susijusius PII incidentus, netinkamą naudojimą, neautorizuotą atskleidimą ir nepalankius privatumo rezultatus per REG10 ir REG12;
- 3.1.9 registruoti stebėseną, išimtis, neatitiktis, korekcinius veiksmus ir patobulinimus REG12.

### 4. Politikos nuostatos

#### 4.1 DI, profiliavimo ir automatizuoto sprendimų priėmimo identifiкуavimas

- 4.1.1 [Controller] Kai siūloma nauja arba iš esmės pakeista sistema, taikomoji programa, modelis, darbo eiga, paslauga ar verslo procesas, Process Owner / Business Owner turi nustatyti, ar jis naudoja DI, profiliavimą, vertinimą balais, rekomendavimą, sprendimų priėmimo paramą ar automatizuotą sprendimų priėmimą, susijusį su PII, ir užregistruoti nustatymą REG02.
- 4.1.2 [Controller] Prieš pradėdamas su DI susijusį PII tvarkymą, Process Owner / Business Owner turi REG02 dokumentuoti tvarkymo tikslą, PII kategorijas, duomenų subjektų kategorijas, duomenų šaltinius, numanomų ar išvestinių duomenų kategorijas, išvesties kategorijas, gavėjų kategorijas, teisinį pagrindą ir saugojimo sąsają.
- 4.1.3 [Controller] Prieš naudojant profiliavimą, vertinimą balais, rekomendavimą, sprendimų priėmimo paramą ar automatizuotą sprendimų priėmimą produkcinėje aplinkoje, Process Owner / Business Owner turi REG02 ir REG04 dokumentuoti sprendimo kontekstą, numatomą poveikį duomenų subjektams, žmogaus dalyvavimą ir teisių įgyvendinimo kelią.
- 4.1.4 [Joint Controller] Prieš atliekant su DI susijusį PII tvarkymą kartu su bendru duomenų valdytoju, Privacy Lead / PIMS Manager turi REG08 dokumentuoti atsakomybę už tikslo apibrėžimą, pranešimą, teisių tvarkymą, DPIA palaikymą, duomenų tvarkytojų valdyseną ir incidentų eskalavimą.
- 4.1.5 [Processor] Prieš tvarkydamas PII per su DI susijusią paslaugą klientui, Process Owner / Business Owner turi patvirtinti, kad kliento nurodymai, leidžiami tikslai, draudžiami naudojimo būdai, išvesties tvarkymas ir pagalbos pareigos yra dokumentuoti REG08.

4.1.6 [Both] Prieš aktyvuojant su DI susijusį PII tvarkymą, Privacy Lead / PIMS Manager turi patvirtinti, kad tvarkymas susietas su taikytiniais kanoniniais įrodymų objektais ir kad už REG02, REG04, REG06, REG07, REG08, REG09, REG10 ar REG12 ribų nesukuriamas atskiras DI skirtas registras.

#### **4.2 Privatumo rizikos vertinimas ir DPIA nukreipimas**

4.2.1 [Controller] Prieš paleidžiant arba iš esmės keičiant su DI susijusį PII tvarkymą, Privacy Lead / PIMS Manager turi atlikti pirminį privatumo rizikos vertinimą ir REG04 užregistruoti sprendimą dėl DPIA.

4.2.2 [Conditional] Kai su DI susijęs tvarkymas apima profiliavimą, automatizuotus sprendimus, didelio masto vertinimą, specialių kategorijų duomenis, nusikalstamų veikų duomenis, pažeidžiamus duomenų subjektus, darbuotojų vertinimą, vaikus, elgsenos stebėseną, vietos duomenis, biometrinius duomenis, didelio poveikio vertinimą balais arba reikšmingą poveikį, Data Protection Officer / Privacy Advisor turi peržiūrėti privatumo riziką ir REG04 užregistruoti konsultaciją.

4.2.3 [Controller] Prieš su DI susijusio PII tvarkymo paleidimą į produkcinę aplinką, Process Owner / Business Owner turi REG04 arba REG12 dokumentuoti rizikos tvarkymo veiksmus, liekamosios rizikos būseną ir pasirengimo paleidimui įrodymus.

4.2.4 [Controller] Prieš pakartotinai naudojant PII DI mokymui, testavimui, validavimui, derinimui, stebėsenai ar modelio tobulinimui nauju arba iš esmės pakeistu tikslu, Process Owner / Business Owner turi atlikti privatumo peržiūrą ir REG02 bei REG04 užregistruoti sprendimą.

4.2.5 [Conditional] Kai po suplanuoto tvarkymo išlieka didelė liekamoji privatumo rizika, Top Management turi patvirtinti, atmesti arba pareikalauti papildomo tvarkymo prieš naudojimą produkcinėje aplinkoje ir REG04 bei REG12 užregistruoti sprendimą.

[ ... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ... ]

### **9. Išimties**

9.1 [All] Prieš nukrypdamas nuo su DI susijusio privatumo reikalavimo šioje politikoje, prašymą teikiantis Process Owner / Business Owner turi REG12 pateikti išimties pagrindimą ir kompensuojančių kontrolės priemonių įrodymus.

9.2 [Conditional] Kai išimtis paveikia profiliavimą, automatizuotą sprendimų priėmimą, žmogaus atliekamą peržiūrą, sprendimo užginčijimą, skaidrumą, DPIA rezultatą, didelio poveikio vertinimą balais, su vaikais susijusį tvarkymą, su darbuotojais susijusį tvarkymą, duomenų tvarkytojo apribojimus ar tarptautinius perdavimus, Data Protection Officer / Privacy Advisor turi peržiūrėti išimtį ir REG04 arba REG12 užregistruoti konsultaciją.

9.3 [Conditional] Kai išimtis sukuria arba išlaiko didelę liekamąją privatumo riziką, Top Management turi patvirtinti arba atmesti išimtį ir REG04 bei REG12 užregistruoti sprendimą.

9.4 [All] Prieš pasibaigiant patvirtintos su DI susijusios privatumo išimties galiojimui, Privacy Lead / PIMS Manager turi peržiūrėti uždarymo, pratęsimo ar korekcinį veiksmų būseną ir REG12 užregistruoti rezultatą.

### **10. Politikos laikymosi užtikrinimas**

10.1 [All] Nustačius šios politikos nesilaikymą, Privacy Lead / PIMS Manager turi REG12 užregistruoti neatitiktį ir korekcinį veiksma.

10.2 [Both] Kai įtariamas neautorizuotas su DI susijęs PII tvarkymas, atskleidimas, prieiga, netinkamas modelio naudojimas, teisių neįvykdymas ar nepalankus privatumo rezultatas, Incident Response Coordinator turi inicijuoti incidento eskalavimą ir REG10 bei REG12 užregistruoti įrodymus.

- 10.3 [Both] Kai duomenų tvarkytojas, subtvarkytojas, tiekėjas ar duomenų dalijimosi gavėjas neįvykdo su DI susijusių privatumo pareigų, Vendor / Procurement Owner turi REG08 ir REG12 užregistruoti taisomąjį, eskalavimo arba nutraukimo veiksmą.
- 10.4 [All] Kai pasikartoja arba sistemškai atsiranda su DI susijusių privatumo neatitikčių, Top Management turi peržiūrėti klausimą ir REG12 užregistruoti vadovybės veiksmą.

#### **11. Peržiūra ir priežiūra**

- 11.1 [All] Bent kartą per metus Privacy Lead / PIMS Manager turi peržiūrėti šią politiką dėl nuolatinio tinkamumo ir REG12 užregistruoti peržiūros rezultata.
- 11.2 [Conditional] Kai teisės aktai, paslaugos, modeliai, duomenų šaltiniai, profiliavimo praktika, automatizuoto sprendimų priėmimo logika, tiekėjų susitarimai, perdavimo keliai ar privatumo rizikos iš esmės pasikeičia, Privacy Lead / PIMS Manager turi peržiūrėti paveiktas su DI susijusias privatumo kontrolės priemones ir REG02, REG04 arba REG12 užregistruoti rezultata.
- 11.3 [Controller] Bent kartą per metus ir po esminių su DI susijusios naudotojo kelionės pakeitimų Process Owner / Business Owner turi peržiūrėti skaidrumo, prasmingos informacijos, žmogaus atliekamos peržiūros ir teisių įgyvendinimo kelio įrodymus ir REG06 bei REG07 užregistruoti peržiūrą.
- 11.4 [All] Uždarius su DI susijusius privatumo korekcinis veiksmus, Internal Audit / Compliance Reviewer turi patikrinti veiksmingumą ir REG12 užregistruoti patikrinimo įrodymus.

#### **12. Susijusios politikos**

- 12.1 PII01 - Privačios informacijos apsaugos valdymo sistemos politika
- 12.2 PII02 - Privatumo vaidmenų, atsakomybių ir atskaitomybės politika
- 12.3 PII03 - PII tvarkymo veiklos apskaitos ir teisinio pagrindo politika
- 12.4 PII04 - Privatumo pranešimų ir skaidrumo politika
- 12.5 PII05 - Sutikimų ir nuostatų valdymo politika
- 12.6 PII06 - Duomenų subjektų teisių valdymo politika
- 12.7 PII07 - Privatumo rizikos vertinimo ir DPIA politika
- 12.8 PII08 - Privatumo pagal projektavimą ir pagal numatytuosius nustatymus politika
- 12.9 PII09 - PII rinkimo, naudojimo, atskleidimo ir dalijimosi politika
- 12.10 PII10 - PII saugojimo, ištrynimo ir sunaikinimo politika
- 12.11 PII11 - PII tikslumo ir kokybės politika
- 12.12 PII12 - Duomenų tvarkytojų, subtvarkytojų ir trečiųjų šalių privatumo valdymo politika
- 12.13 PII13 - Tarptautinio PII perdavimo politika
- 12.14 PII14 - PII saugumo ir prieigos kontrolės politika
- 12.15 PII15 - PII incidentų ir pažeidimų valdymo politika
- 12.16 PII17 - PIMS dokumentuotos informacijos ir įrodymų valdymo politika
- 12.17 PII18 - PIMS stebėsenos, audito ir tobulinimo politika
- 12.18 PII19 - Darbuotojų privatumo politika
- 12.19 PII20 - Vaikų privatumo politika
- 12.20 PII22 - Rinkodaros privatumo ir slapukų politika

#### **13. Pamatiniai standartai ir sistemos**

- 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].