					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII21					Asiakirjan nimi: **Tekoälyn ja automaattisen päätöksenteon tietosuojapolitiikka**							
Versio: 1.0		Voimaantulopäivä: 01.01.2025			Asiakirjan omistaja:							
X	Politiikka		Standardi		Menettely		Lomake		Rekisteri		Muu	

Muutoshistoria				
Muutosnumero	**Muutospäivä**	**Muutokset**	**Tarkistanut**	**Prosessin omistaja**

Hyväksynnät			
Nimi	**Tehtävänimike**	**Päivämäärä**	**Allekirjoitus**

Yhdenmukaisuus standardien ja säädösten kanssa

Standardi / säädös	Lauseke / hallintakeino / artikla	Soveltuvuus	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentoitu tieto ja operatiivinen ohjaus tekoälyyn, profilointiin ja automaattiseen päätöksentekoon liittyvän käsittelyn todentavaa aineistoa varten
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Tekoälyn tietosuojakontrollien seuranta, poikkeamat ja korjaavat toimenpiteet
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	Tarkoitus, oikeusperuste, tietosuojaa koskeva vaikutustenarviointi ja rekisterinpitäjän tallenteet
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Henkilötietojen käsittelijöitä koskevat sopimukset ja yhteisrekisterinpitäjien vastuut tekoälyyn liittyvässä PII:n käsittelyssä
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Velvoitteet rekisteröityjä kohtaan ja läpinäkyvyys tekoälyyn liittyvässä käsittelyssä
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	Vastustaminen, pääsy tietoihin, oikaisu, poistaminen, pyyntöjen käsittely ja automaattista päätöksentekoa koskevat velvoitteet
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Keräämisen, käsittelyn ja minimoinnin rajat tekoälyn syötteille, tuotoksille ja johdetuille tiedoille
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	Tekoälyyn liittyvän PII:n kansainvälisen siirron, luovutuksen ja luovutuspyyntöjen reititys
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	Henkilötietojen käsittelijän sopimus, dokumentoidut ohjeet, asiakkaan velvoitteiden tuki ja tallenteet

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	Henkilötietojen käsittelijän tuki rekisteröityjä koskeville velvoitteille, siirtojen reititys ja luovutusten käsittely
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Tekoälyyn liittyvän PII:n käsittelyä koskevien tallenteiden ja lokituksen suojaaminen
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	Profilointi, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, minimointi, täsmällisyys ja osoitusvelvollisuus
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Lainmukaisuus, erityisiin henkilötietoryhmiin kuuluvat tiedot sekä rikostuomioihin tai rikkomuksiin liittyvien tietojen suojatoimet
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Läpinäkyvä informointi, pääsy tietoihin ja merkitykselliset tiedot automaattisesta päätöksenteosta
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Oikaisu, poistaminen, käsittelyn rajoittaminen, vastustaminen ja automaattista päätöksentekoa koskevat oikeudet
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Rekisterinpitäjän vastuu, sisäänrakennettu ja oletusarvoinen tietosuoja, yhteisrekisterinpitäjät, henkilötietojen käsittelijät, tallenteet, turvallisuus, DPIA ja tietosuojavastaavan tehtävät
GDPR	Article 44	Conditional	Referenced	Tekoälyyn liittyvän PII:n käsittelyn kansainvälisen siirron reititys
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Tarkoitusta, keräämistä, minimointia, käyttöä, säilytystä, luovutusta, täsmällisyyttä ja laatua koskevat periaatteet

ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Läpinäkyvyys, yksilön osallistuminen, osoitusvelvollisuus, tietoturva ja tietosuojan vaatimustenmukaisuus
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA:n hyöty, kynnysarvon määrittäminen ja valmistautuminen tekoälyyn liittyvien tietosuojariskien arviointiin
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Tarkoitusta, keräämistä, minimointia, käyttöä, säilytystä, luovutusta, täsmällisyyttä ja rekisteröityjen osallistumista koskevat kontrollit

1. Soveltamisala

1.1 Tämä politiikka määrittää pakolliset tietosuojavaatimukset tekoälyä, profilointia, pisteytystä, suosittelua, päätöksenteon tukea ja automaattista päätöksentekoa koskeville käsittelytoimille, joissa käytetään, päätellään, tuotetaan, luovutetaan tai muutoin käsitellään PII:tä PIMS:n soveltamisalassa.

1.2 Tätä politiikkaa sovelletaan seuraaviin:

1.2.1 tekoälyä hyödyntävät järjestelmät, sovellukset, mallit, palvelut, työnkulut, päätöksentekomoottorit, pisteytystyökalut, suosittelujärjestelmät, analytiikkamallit ja automaattisen päätöksenteon prosessit, jotka käsittelevät PII:tä;

1.2.2 profilointi, segmentointi, luokittelu, ennustaminen, päättely, personointi, järjestykseen asettaminen, kelpoisuuden arviointi, petostentorjunta, riskipisteytys, pääsyä koskevat päätökset, työsuhteeseen liittyvä arviointi, lapsiin liittyvä profilointi, markkinoinnin personointi ja vastaava käsittely, jossa PII on mukana;

1.2.3 tekoälyyn liittyvä PII, jota käytetään koulutukseen, testaukseen, validointiin, hienosäätöön, seurantaan, tuotantopäättelyyn, tuotosten arviointiin, suorituskyvyn mittaamiseen, poikkeamien tutkintaan tai mallin käytöstä poistamiseen;

1.2.4 rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän kontekstit;

1.2.5 tekoälyyn liittyvät toimittajat, henkilötietojen käsittelijät, alikäsittelijät, tietojen jakamisen vastaanottajat ja kansainväliset siirtoreitit, jotka käsittelevät PII:tä.

1.3 Tämä politiikka ei luo kattavaa tekoälyn hallinnointikehystä, tekoälyn hallintajärjestelmää, tekoälyinventaaria, mallien inventaaria, malliriskirekisteriä, kohtuullisuusrekisteriä, algoritmirekisteriä, tekoälypoikkeamien rekisteriä, tekoälykomiteaa, mallinomistajan roolia, tekoälyjärjestelmän omistajan roolia, oikeudellisen neuvonnan työnkulkua tai erillistä tekoälyn hyväksyntälomaketta.

1.4 Tämä politiikka ei korvaa seuraavia:

1.4.1 PII03 käsittelytoimien luetteloa, oikeusperustetta ja ROPA:n omistajuutta varten;

1.4.2 PII04 tietosuojaselosteiden hallinnointia varten;

1.4.3 PII05 suostumuksen ja valinta-asetusten hallintaa varten;

1.4.4 PII06 rekisteröidyn oikeuksia koskevaa työnkulkua varten;

1.4.5 PII07 tietosuojariskien arviointia ja DPIA-menetelmää varten;

1.4.6 PII08 sisäänrakennetun ja oletusarvoisen tietosuojan portteja varten;

1.4.7 PII09 keräämisen, käytön, luovutuksen ja jakamisen kontrolleja varten;

1.4.8 PII10 säilytyksen, poistamisen ja hävittämisen toteuttamista varten;

1.4.9 PII11 täsmällisyyden ja laadun kontrolleja varten;

1.4.10 PII12 henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten elinkaaren hallinnointia varten;

1.4.11 PII13 kansainvälisten siirtojen kontrolleja varten;

1.4.12 PII14 turvallisuutta ja pääsynhallintaa varten;

1.4.13 PII15 poikkeamien ja tietoturvaloukkausten käsittelyä varten;

1.4.14 PII18 seurantaa, auditointia ja parantamista varten;

1.4.15 PII19 työntekijöiden tietosuojaa varten;

1.4.16 PII20 lasten tietosuojaa varten;

1.4.17 PII22 markkinoinnin tietosuojaa ja evästeitä varten.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että tekoälyyn, profilointiin ja automaattiseen päätöksentekoon liittyvät PII:tä koskevat toimet tunnistetaan, dokumentoidaan, arvioidaan riskien osalta, toteutetaan läpinäkyvästi ja riitautettavasti, niitä seurataan ja niitä hallitaan PIMS:n kautta ilman päällekkäisten tekoälykohtaisten hallinnointiaineistojen luomista.

2.2 Tämä politiikka varmistaa, että tekoälyyn liittyvän PII:n käsittelyä koskevat tietosuojavelvoitteet todennetaan REG02:n, REG04:n, REG06:n, REG07:n, REG08:n, REG09:n, REG10:n ja REG12:n kautta.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 tunnistaa tekoälyyn, profilointiin ja automaattiseen päätöksentekoon liittyvä PII:n käsittely REG02:ssa;

3.1.2 dokumentoida tekoälyyn liittyvät tarkoitukset, oikeusperuste, PII-luokat, tietolähteet, päätellyt tiedot, tuotokset, vastaanottajat ja päätösten vaikutukset REG02:ssa;

3.1.3 käynnistää tietosuojariskien esiarviointi ja DPIA-reititys REG04:n kautta;

3.1.4 varmistaa, että tekoälyyn liittyvät tietosuojaselosteet ja merkitykselliset tiedot kirjataan REG07:ään;

3.1.5 reitittää oikeuksia, vastustamista, ihmisen suorittamaa uudelleentarkastelua ja riitautettavuutta koskevat pyynnöt REG06:n kautta;

3.1.6 hallita tekoälyyn liittyviä henkilötietojen käsittelijöitä, alikäsittelijöitä, toimittajia ja tietojen jakamisjärjestelyjä REG08:n kautta;

3.1.7 reitittää tekoälyyn liittyvät kansainväliset siirrot REG09:n kautta;

3.1.8 eskaloida epäillyt tekoälyyn liittyvät henkilötietopoikkeamat, väärinkäyttö, luvaton luovutus ja haitalliset tietosuojatulokset REG10:n ja REG12:n kautta;

3.1.9 kirjata seuranta, poikkeukset, poikkeamat, korjaavat toimenpiteet ja parannukset REG12:een.

4. Politiikkalausumat

4.1 Tekoälyn, profiloinnin ja automaattisen päätöksenteon tunnistaminen

4.1.1 [Controller] Kun uutta tai olennaisesti muutettua järjestelmää, sovellusta, mallia, työnkulkua, palvelua tai liiketoimintaprosessia ehdotetaan, roolin Process Owner / Business Owner tulee määrittää, käyttääkö se tekoälyä, profilointia, pisteytystä, suosittelua, päätöksenteon tukea tai automaattista päätöksentekoa, johon liittyy PII:tä, ja kirjata määritys REG02:een.

4.1.2 [Controller] Ennen tekoälyyn liittyvän PII:n käsittelyn aloittamista roolin Process Owner / Business Owner tulee dokumentoida käsittelyn tarkoitus, PII-luokat, rekisteröityjen luokat, tietolähteet, päätellyt tai johdetut tietoluokat, tuotosluokat, vastaanottajaluokat, oikeusperuste ja säilytysyhteys REG02:ssa.

4.1.3 [Controller] Ennen kuin profilointia, pisteytystä, suosittelua, päätöksenteon tukea tai automaattista päätöksentekoa käytetään tuotannossa, roolin Process Owner / Business Owner tulee dokumentoida päätöksentekokonteksti, odotettu vaikutus rekisteröityihin, ihmisen osallistuminen ja oikeuksien käyttämisen reitti REG02:ssa ja REG04:ssä.

4.1.4 [Joint Controller] Ennen kuin tekoälyyn liittyvää PII:n käsittelyä tehdään yhteisrekisterinpitäjän kanssa, roolin Privacy Lead / PIMS Manager tulee dokumentoida vastuu tarkoituksen määrittelystä, tietosuojaselosteesta, oikeuksien käsittelystä, DPIA-tuesta, henkilötietojen käsittelijöiden hallinnoinnista ja poikkeamien eskaloinnista REG08:ssa.

4.1.5 [Processor] Ennen PII:n käsittelyä asiakkaalle tuotettavan tekoälyyn liittyvän palvelun kautta roolin Process Owner / Business Owner tulee vahvistaa, että asiakkaan ohjeet, sallitut

tarkoitukset, kielletyt käyttötavat, tuotosten käsittely ja avustamisvelvoitteet on dokumentoitu REG08:ssa.

4.1.6 [Both] Ennen tekoälyyn liittyvän PII:n käsittelyn aktivointia roolin Privacy Lead / PIMS Manager tulee vahvistaa, että käsittely on linkitetty sovellettaviin kanonisiin näyttöobjekteihin ja että erillistä tekoälykohtaista rekisteriä ei luoda REG02:n, REG04:n, REG06:n, REG07:n, REG08:n, REG09:n, REG10:n tai REG12:n ulkopuolelle.

4.2 Tietosuojariskien arviointi ja DPIA-reititys

4.2.1 [Controller] Ennen tekoälyyn liittyvän PII:n käsittelyn käynnistämistä tai olennaista muuttamista roolin Privacy Lead / PIMS Manager tulee suorittaa tietosuojariskien esiarviointi ja kirjata DPIA-päätös REG04:ään.

4.2.2 [Conditional] Kun tekoälyyn liittyvä käsittely sisältää profilointia, automaattisia päätöksiä, laajamittaista arviointia, erityisiin henkilötietoryhmiin kuuluvia tietoja, rikostuomioihin tai rikkomuksiin liittyviä tietoja, haavoittuvassa asemassa olevia rekisteröityjä, työntekijöiden arviointia, lapsia, käyttäytymisen seurantaa, sijaintitietoja, biometrisiä tietoja, vaikutuksiltaan merkittävää pisteytystä tai merkittäviä vaikutuksia, roolin Data Protection Officer / Privacy Advisor tulee arvioida tietosuojariski ja kirjata neuvo REG04:ään.

4.2.3 [Controller] Ennen tekoälyyn liittyvän PII:n käsittelyn tuotantokäyttöönottoa roolin Process Owner / Business Owner tulee dokumentoida riskien käsittelytoimet, jäännösriskin tila ja tuotantokäyttöönoton valmiutta koskeva todentava aineisto REG04:ssä tai REG12:ssa.

4.2.4 [Controller] Ennen kuin PII:tä käytetään uudelleen tekoälyn koulutukseen, testaukseen, validointiin, hienosäätöön, seurantaan tai mallin parantamiseen uutta tai olennaisesti muutettua tarkoitusta varten, roolin Process Owner / Business Owner tulee suorittaa tietosuojakatselmointi ja kirjata päätös REG02:een ja REG04:ään.

4.2.5 [Conditional] Kun tietosuojaan kohdistuva jäännösriski säilyy korkeana suunnitellun käsittelyn jälkeen, roolin Top Management tulee hyväksyä tai hylätä tuotantokäyttö tai edellyttää lisäkäsittelyä ennen tuotantokäyttöä ja kirjata päätös REG04:ään ja REG12:een.

[... Jaksot 4.3–8 eivät sisälly tähän esikatseluun. Osta koko asiakirja saadaksesi täyden sisällön. ...]

9. Poikkeukset

9.1 [All] Ennen tästä politiikasta johtuvasta tekoälyyn liittyvästä tietosuojavaatimuksesta poikkeamista pyynnön esittävän roolin Process Owner / Business Owner tulee toimittaa poikkeuksen perustelu ja korvaavien kontrollien todentava aineisto REG12:een.

9.2 [Conditional] Kun poikkeus vaikuttaa profilointiin, automaattiseen päätöksentekoon, ihmisen suorittamaan uudelleentarkasteluun, riitautettavuuteen, läpinäkyvyyteen, DPIA:n tulokseen, vaikutuksiltaan merkittävään pisteytykseen, lapsiin liittyvään käsittelyyn, työntekijöihin liittyvään käsittelyyn, henkilötietojen käsittelijän rajoituksiin tai kansainvälisiin siirtoihin, roolin Data Protection Officer / Privacy Advisor tulee arvioida poikkeus ja kirjata neuvo REG04:ään tai REG12:een.

9.3 [Conditional] Kun poikkeus luo tai säilyttää korkean tietosuojaan kohdistuvan jäännösriskin, roolin Top Management tulee hyväksyä tai hylätä poikkeus ja kirjata päätös REG04:ään ja REG12:een.

9.4 [All] Ennen hyväksytyn tekoälyyn liittyvän tietosuojapoikkeuksen päättymistä roolin Privacy Lead / PIMS Manager tulee arvioida sulkemisen, uusimisen tai korjaavan toimenpiteen tila ja kirjata tulos REG12:een.

10. Soveltaminen

10.1 [All] Kun tämän politiikan noudattamatta jättäminen tunnistetaan, roolin Privacy Lead / PIMS Manager tulee kirjata poikkeama ja korjaava toimenpide REG12:een.

10.2 [Both] Kun epäillään luvatonta tekoälyyn liittyvän PII:n käsittelyä, luovutusta, pääsyä, mallin väärinkäyttöä, oikeuksien toteuttamisen epäonnistumista tai haitallista tietosuojatulosta, roolin

Incident Response Coordinator tulee käynnistää poikkeaman eskalointi ja kirjata todentava aineisto REG10:een ja REG12:een.

10.3 [Both] Kun henkilötietojen käsittelijä, alikäsittelijä, toimittaja tai tietojen jakamisen vastaanottaja ei täytä tekoälyyn liittyviä tietosuojavelvoitteita, roolin Vendor / Procurement Owner tulee kirjata korjaaminen, eskalointi tai päättämistoimi REG08:aan ja REG12:een.

10.4 [All] Kun toistuvia tai järjestelmällisiä tekoälyyn liittyviä tietosuojapoikkeamia ilmenee, roolin Top Management tulee arvioida asia ja kirjata johdon toimenpide REG12:een.

11. Katselmointi ja ylläpito

11.1 [All] Vähintään vuosittain roolin Privacy Lead / PIMS Manager tulee katselmoida tämän politiikan jatkuva soveltuvuus ja kirjata katselmoinnin tulos REG12:een.

11.2 [Conditional] Kun lait, palvelut, mallit, tietolähteet, profilointikäytännöt, automaattisen päätöksenteon logiikka, toimittajajärjestelyt, siirtoreitit tai tietosuojariskit muuttuvat olennaisesti, roolin Privacy Lead / PIMS Manager tulee arvioida vaikutuksen kohteena olevat tekoälyyn liittyvät tietosuojakontrollit ja kirjata tulos REG02:een, REG04:ään tai REG12:een.

11.3 [Controller] Vähintään vuosittain ja olennaisten tekoälyyn liittyvien käyttäjäpolun muutosten jälkeen roolin Process Owner / Business Owner tulee arvioida läpinäkyvyyttä, merkityksellisiä tietoja, ihmisen suorittamaa uudelleentarkastelua ja oikeuksien käyttämisen reittiä koskeva todentava aineisto sekä kirjata arviointi REG06:een ja REG07:ään.

11.4 [All] Kun tekoälyyn liittyvät tietosuojan korjaavat toimenpiteet on suljettu, roolin Internal Audit / Compliance Reviewer tulee varmentaa vaikuttavuus ja kirjata varmennuksen todentava aineisto REG12:een.

12. Liittyvät politiikat

12.1 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.2 PII02 - Tietosuojan rooleja, vastuita ja osoitusvelvollisuutta koskeva politiikka

12.3 PII03 - PII:n käsittelytoimien luetteloa ja oikeusperustetta koskeva politiikka

12.4 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.5 PII05 - Suostumuksen ja valinta-asetusten hallintapolitiikka

12.6 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.7 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.8 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.9 PII09 - PII:n keräämistä, käyttöä, luovutusta ja jakamista koskeva politiikka

12.10 PII10 - PII:n säilytys-, poistamis- ja hävittämispolitiikka

12.11 PII11 - PII:n täsmällisyys- ja laatupolitiikka

12.12 PII12 - Henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojahallinnan politiikka

12.13 PII13 - PII:n kansainvälisten siirtojen politiikka

12.14 PII14 - PII:n turvallisuus- ja pääsynhallintapolitiikka

12.15 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.16 PII17 - PIMS:n dokumentoitujen tietojen ja todentavan aineiston hallintapolitiikka

12.17 PII18 - PIMS:n seuranta-, auditointi- ja parantamispolitiikka

12.18 PII19 - Työntekijöiden tietosuojapolitiikka

12.19 PII20 - Lasten tietosuojapolitiikka

12.20 PII22 - Markkinoinnin tietosuoja- ja evästepolitiikka

13. Viitestandardit ja viitekehykset

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].