					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII23					Asiakirjan nimi: **Pilvipalvelujen PII:n käsittelijäpolitiikka**							
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	Kohta / kontrolli / artikla	Sovellettavuus	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	PIMS-rooli ja kontrollien sovellettavuus
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentoitu pilvipalvelun käsittelijää koskeva todentava aineisto ja operatiivinen ohjaus
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Seuranta, poikkeamat ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Asiakassopimukset, ohjeet, tuki ja tallenteet
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Asiakkaan avustaminen rekisteröityä koskevissa velvoitteissa
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Väliaikaiset tiedostot, palautus, siirto, hävitys ja siirron kontrollit
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Siirtoperuste ja sijainnit
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Luovutusten tallenteet ja luovutuspyyntöjen käsittely
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Alikäsittelijöiden ilmoittaminen, käyttöön ottaminen ja muutoksista ilmoittaminen
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Pääsyä, tallenteita, varmuuskopiointia ja lokitusta koskeva todentava aineisto
GDPR	Article 28	Processor	Primary	Käsittelijä, alikäsittelijä, avustaminen, auditointi, poistaminen ja palauttaminen

GDPR	Article 30	Processor	Supporting	Käsittelijän tallenteet
GDPR	Article 32; Article 33	Processor	Supporting	Turvallisuus ja tietoturvaloukkauksesta ilmoittaminen rekisterinpitäjälle
GDPR	Article 44	Conditional	Referenced	Kansainvälisen siirron reititys
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Käyttötarkoituksen, minimoinnin, käytön, säilytyksen ja luovutuksen rajoittaminen
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Osoitusvelvollisuus, tietoturva ja vaatimustenmukaisuus
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Käsittelijän arviointi, seuranta, muutos ja säilytyskontrollit
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Kontrollien sovellettavuus, operatiivinen ohjaus sekä toimittaja- ja pilvikontrollit
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Toimittaja-, pilvi-, poistamis-, lokitus- ja seurantakontrollit
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Pilvipalvelun käsittelijän asiakasavustus ja käyttötarkoituksen rajoittaminen
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Pilvipalvelujen luovutusilmoitukset, luovutustallenteet ja alikäsittelijöiden läpinäkyvyys
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Pilvipalvelujen tietoturvaloukkausten rajapinta, exit, sopimustoimet,

				alikäsittelysopimukset ja sijaintitallenteet
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Toimitussuhdestrategia ja hallinnointi
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Toimittajasuhteen suunnittelu, sopimus, hallinta, seuranta ja päättäminen
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Poistamisen viitekehys ja dokumentointi
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Poistamisen toteutus ja poikkeukset

1. Soveltamisala

1.1 Tässä politiikassa määritetään pakolliset tietosuojavaatimukset pilvipalveluille, joissa organisaatio toimii PII:n käsittelijänä tai alikäsittelijänä, mukaan lukien SaaS-, PaaS- ja IaaS-palvelut, isännöidyt sovellukset, hallinnoidut pilvipalvelut, pilvituki, pilvitallennus, pilvianalytiikka ja pilvi-infrastruktuuripalvelut, jotka käsittelevät PII:tä asiakkaiden puolesta.

1.2 Tätä politiikkaa sovelletaan pilvessä tapahtuvaan käsittelyyn, joka tehdään asiakassopimusten, dokumentoitujen asiakkaan ohjeiden, ylemmän tason käsittelijän ohjeiden, alikäsittelijäjärjestelyjen, pilvialueen konfiguraation, pilvituen pääsyn, palvelun ylläpidon, varmuuskopioinnin, replikoinnin, lokituksen, seurannan, poistamisen, palauttamisen, tietoturvaloukkauksen tuen, auditointituen ja asiakkaan avustamisvelvoitteiden perusteella.

1.3 Tämä politiikka kattaa:

1.3.1 pilvessä tapahtuvan PII:n käsittelyn soveltamisalan ja ohjekirjaukset;

1.3.2 asiakassopimuksen ja jaetun vastuun todentavan aineiston;

1.3.3 tenanttien eristämisen, pilvipalveluun pääsyn, ylläpidollisen pääsyn ja lokitusta koskevan todentavan aineiston;

1.3.4 alikäsittelijöiden ja pilvitoimitusketjun hallinnoinnin;

1.3.5 sijainnin, etäkäytön ja henkilötietojen kansainvälisen siirron reitityksen;

1.3.6 palauttamista, siirtämistä, poistamista, hävittämistä ja päättämisvaihetta koskevan todentavan aineiston;

1.3.7 asiakkaan avustamisen rekisteröidyn oikeuksissa, DPIA-vaikutustenarvioinneissa, auditoinneissa ja tietoturvaloukkauksiin reagoinnissa;

1.3.8 seuranta-, poikkeus-, soveltamis- ja parantamisaineiston.

1.4 Tämä politiikka ei luo erillistä asiakassopimusrekisteriä, pilvipalvelurekisteriä, tenanttien eristämisrekisteriä, pääsyrekisteriä, lokirekisteriä, poistamisrekisteriä, tukipyyntörekisteriä, auditointinäyttörekisteriä, tietoturvaloukkausrekisteriä, alikäsittelijärekisteriä tai pilvihallinnon komiteaa.

1.5 Tämä politiikka ei korvaa:

1.5.1 PII03-politiikkaa käsittelytoimien luettelosta ja oikeusperusteen omistajuudesta;

1.5.2 PII06-politiikkaa rekisteröidyn oikeuksien täysimääräisestä työnkulusta;

1.5.3 PII07-politiikkaa tietosuojariskien ja DPIA:n menetelmästä;

1.5.4 PII08-politiikkaa sisäänrakennetun ja oletusarvoisen tietosuojan porteista;

1.5.5 PII09-politiikkaa keräämisen, käytön, luovuttamisen ja jakamisen yleisistä kontrolleista;

1.5.6 PII10-politiikkaa säilyttämisen, poistamisen ja hävittämisen menetelmästä;

1.5.7 PII12-politiikkaa käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten yleisestä elinkaaren hallinnoinnista;

1.5.8 PII13-politiikkaa kansainvälisen siirtomekanismin arvioinnista;

1.5.9 PII14-politiikkaa PII:n tietoturvan ja pääsynhallinnan kokonaisarkkitehtuurista;

1.5.10 PII15-politiikkaa poikkeamien ja tietoturvaloukkausten hallinnan työnkulusta;

1.5.11 PII17-politiikkaa dokumentoidun tiedon hallinnasta;

1.5.12 PII18-politiikkaa PIMS-seurannan, auditoinnin ja parantamisen hallinnoinnista.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että pilvipalveluina tuotettavat PII:n käsittelijä- ja alikäsittelijäpalvelut toimivat dokumentoitujen asiakkaan ohjeiden, selkeän käsittelyn soveltamisalan, hallittujen alikäsittelijäjärjestelyjen, asianmukaisten pilviturvallisuuden vastuiden, dokumentoidun sijainnin ja siirtoreitityksen, asiakkaan avustamisvelvoitteiden,

tietoturvaloukkauksen tuen, poistamis- ja palautuskyvykkyyden sekä auditointivalmiin todentavan aineiston mukaisesti.

2.2 Tämä politiikka tukee ISO/IEC 27701:2025 -standardin mukaista PIMS-sertifiointivalmiutta pilvipalvelujen käsittelijöille ja alikäsittelijöille siten, että se pysyy integroituna olemassa olevaan PIMS-politiikkakokonaisuuteen ja kanonisiin näyttöobjekteihin.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 Määrittää pilvessä tapahtuvan PII:n käsittelyn soveltamisala ennen asiakkaan käyttöönottoa tai olennaista muutosta.

3.1.2 Varmistaa, että asiakkaan ohjeet kirjataan, katselmoidaan ja niitä noudatetaan.

3.1.3 Ylläpitää pilvipalvelujen käsittelijä- ja alikäsittelijäaineistoa kanonisissa PIMS-rekistereissä.

3.1.4 Määrittää jaetun vastuun, tenanttien eristämisen, pääsyn, lokituksen ja sijainnin todentava aineisto ilman PII:n tietoturvapolitiikan päällekkäisyyttä.

3.1.5 Hallita alikäsittelijöiden käyttöönottoa, muutosta, ketjutettavia velvoitteita ja seurantaa koskevaa todentavaa aineistoa.

3.1.6 Tukea asiakkaita rekisteröidyn oikeuksissa, DPIA-vaikutustenarvioinneissa, auditointipyynnöissä ja tietoturvaloukkauksiin reagoinnissa.

3.1.7 Varmistaa, että palauttamista, poistamista, siirtämistä ja hävittämistä koskeva todentava aineisto säilytetään päättämisvaiheessa.

3.1.8 Seurata pilvipalvelujen käsittelijäkontrolleja ja ohjata korjaavia toimenpiteitä REG12:n avulla.

4. Politiikkalausekkeet

4.1 Pilvikäsittelyn soveltamisala ja asiakkaan ohjeet

4.1.1 [Processor] Privacy Lead / PIMS Manager MUST kirjata jokainen pilvessä tapahtuvan PII:n käsittelypalvelu, asiakkaan käsittelyrooli, asiakkaan ohjeen lähde, PII-luokat, rekisteröityjen ryhmät, palvelun tarkoitus, käsittelysijainti, alikäsittelijäriippuvuus, poistamisriippuvuus ja siirtomerkintä REG02- ja REG08-rekistereihin ennen asiakkaan käyttöönottoa tai olennaista palvelumuutosta.

4.1.2 [Processor] Process Owner / Business Owner MUST kirjata pilvessä tapahtuvaa PII:n käsittelyä koskevat dokumentoidut asiakkaan ohjeet REG08-rekisteriin ennen käsittelyn aloittamista.

4.1.3 [Subprocessor] Process Owner / Business Owner MUST kirjata ylemmän tason käsittelijän tai asiakkaan hyväksymät ohjeet REG08-rekisteriin ennen PII:n käsittelyä pilvipalvelun alikäsittelijänä.

4.1.4 [Processor] Privacy Lead / PIMS Manager MUST kirjata pilvipalvelun käsittelijäkontrollien sovellettavuus REG03-rekisteriin ennen uuden pilvessä tapahtuvan PII:n käsittelypalvelun julkaisua tai olennaista muutosta.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor MUST katselmoida REG12-rekisterissä jokainen asiakkaan ohje, joka vaikuttaa olevan ristiriidassa dokumentoitujen asiakasvelvoitteiden, PIMS-vaatimusten tai hyväksytyn palvelun soveltamisalan kanssa, ennen kuin organisaatio toimii ohjeen perusteella.

4.1.6 [Processor] Process Owner / Business Owner MUST kirjata REG12-rekisteriin kaikki ehdotettu asiakkaan PII:n käsittely, joka tapahtuu dokumentoitujen asiakkaan ohjeiden ulkopuolella, ja hankkia Privacy Lead / PIMS Manager -roolin hyväksyntä ennen käsittelyn tapahtumista.

4.2 Pilvikonfiguraatio, tenanttien eristäminen, pääsy ja lokitus

4.2.1 [Processor] Information Security Lead MUST kirjata pilvipalvelun jaetun vastuun rajaus PII:hin pääsyn, ylläpidon, lokituksen, varmuuskopioinnin, salauksen, haavoittuvuuksien hallinnan ja poistamisen osalta REG08-rekisteriin ennen asiakkaan käyttöönottoa tai olennaista palvelumuutosta.

4.2.2 [Processor] System Owner / Application Owner MUST validoida tenanttien eristäminen tai asiakkaiden erottelukontrollit REG12-rekisterissä ennen tuotantokäyttöä ja olennaisen arkkitehtuurimuutoksen jälkeen.

4.2.3 [Processor] System Owner / Application Owner MUST myöntää ylläpidollinen pääsy asiakkaan PII:hin pilviympäristössä vain sen jälkeen, kun hyväksytty liiketoimintatarve, pääsyn laajuus, pääsyn kesto ja katselmointitiheys on kirjattu REG12-rekisteriin.

4.2.4 [Processor] Information Security Lead MUST katselmoida etuoikeutettu pilvipääsy, tukipääsy, asiakkaan PII:hin pääsy ja lokituksen kattavuus REG12-rekisterissä vähintään neljännesvuosittain.

4.2.5 [Processor] System Owner / Application Owner MUST validoida tuotanto-, staging-, testi- ja tukiympäristöjen erottelu asiakkaan PII:n osalta REG12-rekisterissä ennen julkaisua ja olennaisen ympäristömuutoksen jälkeen.

4.2.6 [Processor] System Owner / Application Owner MUST kirjata asiakkaan PII:tä koskevien varmuuskopioiden, replikoinnin, lokitallennuksen ja tukipääsyn sijainnit REG02-, REG08- tai REG09-rekisteriin ennen kyseisten sijaintien käyttöönottoa tai muuttamista.

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

9. Poikkeukset

9.1 [Processor] Process Owner / Business Owner MUST pyytää pilvipalvelujen käsittelijäpoikkeusta REG12-rekisterissä ennen asiakkaan käyttöönottoa, julkaisua, uusimista tai käytön jatkamista, kun vaadittu asiakkaan ohjeita, alikäsittelijää, sijaintia, pääsyä, lokitusta, poistamista tai poikkeamarajapintaa koskeva todentava aineisto on puutteellinen.

9.2 [Processor] Data Protection Officer / Privacy Advisor MUST katselmoida tietosuojan kannalta merkittävät pilvipalvelujen käsittelijäpoikkeuspyynnöt REG12-rekisterissä ennen hyväksyntää, kun poikkeus vaikuttaa asiakkaan ohjeisiin, rekisteröidyn avustamiseen, siirtoihin, alikäsittelijöihin, poistamiseen, tietoturvaloukkauksen tukeen tai vaikutuksiltaan merkittävään PII:hin.

9.3 [Processor] Top Management MUST hyväksyä korkean riskin tai olennaiset pilvipalvelujen käsittelijäpoikkeukset REG12-rekisterissä ennen poikkeuksen voimaantuloa.

9.4 [Processor] Privacy Lead / PIMS Manager MUST määrittää jokaiselle hyväksytylle pilvipalvelujen käsittelijäpoikkeukselle päättymispäivä, korjaamisesta vastaava omistaja, katselmointipäivä ja jäännösriskiä koskeva huomautus REG12-rekisterissä ennen hyväksyntää.

10. Soveltaminen

10.1 [Processor] Privacy Lead / PIMS Manager MUST estää asiakkaan käyttöönotto, palvelun julkaisu, uusiminen tai käsittelyn jatkaminen, kun vaadittu REG02-, REG03-, REG08-, REG09-, REG10- tai REG12-näyttö puuttuu ennen käsittelyn aloittamista tai jatkamista.

10.2 [Processor] System Owner / Application Owner MUST poistaa hyväksymätön pilvipääsy, hyväksymätön alueen käyttö, hyväksymätön replikointi, hyväksymätön tukipääsy tai hyväksymätön alikäsittelijän tietovirta käytöstä yhden työpäivän kuluessa soveltamispäätöksestä ja kirjata valmistuminen REG08- tai REG12-rekisteriin.

10.3 [Processor] Vendor / Procurement Owner MUST keskeyttää uuden PII:n käsittelyn hyväksymättömän tai vaatimustenvastaisen pilvipalvelun alikäsittelijän toimesta, kunnes REG08-rekisterin korjaavia toimenpiteitä koskeva todentava aineisto on valmis.

10.4 [Processor] Incident Response Coordinator MUST eskaloida asiakkaan poikkeamailmoitusten määräaikojen laiminlyönnit REG10- ja REG12-rekistereissä yhden työpäivän kuluessa tunnistamisesta.

10.5 [Processor] Internal Audit / Compliance Reviewer MUST todentaa korjaavien toimenpiteiden vaikuttavuus merkittävien tai toistuvien pilvipalvelujen käsittelijäpoikkeamien osalta REG12-rekisterissä 60 päivän kuluessa korjaavan toimenpiteen sulkemisesta.

11. Katselmointi ja ylläpito

11.1 [Processor] Privacy Lead / PIMS Manager MUST katselmoida tämä politiikka REG12-rekisterissä vuosittain ja 30 päivän kuluessa olennaisesta muutoksesta, joka koskee pilvipalvelujen käsittelijävelvoitteita, pilviarkkitehtuuria, alikäsittelijöiden hallinnointia, asiakkaan avustamista, poistamiskyvykkyyttä tai sertifiointivaatimuksia.

11.2 [Processor] Vendor / Procurement Owner MUST katselmoida pilvipalvelun alikäsittelijöitä ja pilvipalveluriippuvuuksia koskevat tallenteet REG08-rekisterissä vähintään vuosittain ja ennen uusimista.

11.3 [Processor] System Owner / Application Owner MUST katselmoida tenanttien eristämistä, etuoikeutettua pääsyä, lokitusta, varmuuskopiointia, replikointia ja poistamista koskeva todentava aineisto REG12-rekisterissä vähintään vuosittain ja olennaisen arkkitehtuurimuutoksen jälkeen.

11.4 [Processor] Privacy Lead / PIMS Manager MUST katselmoida REG09-rekisterin pilvisijainti- ja siirtoreititystallenteet vähintään vuosittain ja 15 työpäivän kuluessa olennaisesta sijainti-, tukipääsy-, varmuuskopiointi- tai alikäsittelijämuutoksesta.

11.5 [Processor] Privacy Lead / PIMS Manager MUST päivittää REG03-rekisteri 15 työpäivän kuluessa hyväksytyistä politiikkamuutoksista, jotka vaikuttavat pilvipalvelujen käsittelijäkontrollien sovellettavuuteen.

11.6 [All] Top Management MUST hyväksyä tämän politiikan olennaiset muutokset REG12-rekisterissä ennen julkaisua.

12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.3 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka

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

12.5 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.6 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.7 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.8 PII09 - PII:n keräämistä, käyttöä, luovuttamista ja jakamista koskeva politiikka

12.9 PII10 - PII:n säilyttämis-, poistamis- ja hävittämispolitiikka

12.10 PII12 - Käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten tietosuojahallinnan politiikka

12.11 PII13 - PII:n kansainvälisen siirron politiikka

12.12 PII14 - PII:n tietoturva- ja pääsynhallintapolitiikka

12.13 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.14 PII17 - PIMS-dokumentoidun tiedon ja todentavan aineiston hallintapolitiikka

12.15 PII18 - PIMS-seuranta-, auditointi- ja parantamispolitiikka

12.16 PII20 - Lasten tietosuojapolitiikka

12.17 PII21 - AI- ja automaattisen päätöksenteon tietosuojapolitiikka

12.18 PII22 - Markkinoinnin tietosuoja- ja evästepolitiikka

12.19 PII24 - Kameravalvonnan ja fyysisen seurannan tietosuojapolitiikka

13. Viitestandardit ja viitekehykset

13.1 Tämä politiikka on kartoitettu seuraaviin standardeihin ja säädöksiin. Kartoitus selittää, miten politiikka tukee viitattuja vaatimuksia, ja yksilöi sisäiset kohdat, joilla ne toteutetaan tai joita ne tukevat.

13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].