					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII24					Asiakirjan nimi: **Kameravalvonnan ja fyysisen valvonnan 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	Sovellettavuus	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentoidut ja operatiiviset kontrollit
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seuranta 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, riskiperusteinen heräte ja tallenteet
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Henkilötietojen käsittelijän ja yhteisrekisterinpitäjän vastuunjako
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Rekisteröityä koskevat velvoitteet ja pyynnöt
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	Controller	Primary	Kerääminen, käsittely, minimointi, säilytys ja hävittäminen
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Luovutuksia koskevat tallenteet ja pyynnöt
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	Supporting	Henkilötietojen käsittelijän sopimukset, ohjeet, tuki ja tallenteet
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	Henkilötietojen käsittelijän oikeudet ja luovutustuki
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Tallenteiden suojaus ja lokitus
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Periaatteet ja osoitusvelvollisuus
GDPR	Article 6	Controller	Primary	Oikeusperuste
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Läpinäkyvyys ja tietosuojaselosteet

GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Oikeuksia koskevat pyynnöt
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Hallinnointi, henkilötietojen käsittelijät, tallenteet, turvallisuus, DPIA ja neuvonta
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Tarkoitus, kerääminen, minimointi, säilytys ja luovuttaminen
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Läpinäkyvyys, osallistuminen, osoitusvelvollisuus, turvallisuus ja vaatimustenmukaisuus
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Tietosuojariski ja DPIA-herätteet
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Henkilötietojen suojaamisen tietosuojakontrollit
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Käyttöoikeuksien ja fyysisen sisäänpääsyn hallintakeinot
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, fyysinen valvonta, pääsyn rajoittaminen ja lokitus

1. Soveltamisala

1.1 Tätä politiikkaa sovelletaan kameravalvontaan, videovalvontaan, vierailijoiden valvontaan, fyysisen pääsynhallinnan lokeihin, vartiointihenkilöstön ylläpitämiin valvontatallenteisiin, toimitilojen valvontajärjestelmiin ja niihin liittyviin fyysisen valvonnan toimintoihin, joissa kerätään tai muutoin käsitellään PII:tä.

1.2 Tätä politiikkaa sovelletaan organisaatioihin, jotka toimivat rekisterinpitäjinä omien toimitilojensa ja fyysisen valvonnan toimintojensa osalta. Sitä sovelletaan myös henkilötietojen käsittelijän tai alikäsittelijän tukitoimiin, joissa organisaatio käyttää, ylläpitää, katselmoi, säilyttää, luovuttaa, poistaa tai muutoin käsittelee valvontatallenteita, vierailijatietoja tai fyysisen pääsyn lokeja asiakkaan puolesta.

1.3 Tämä politiikka kattaa valvonnan tarkoituksen määrittelyn, hyväksynnän, ilmoitukset ja valvontakyltit, pääsyn rajoitukset, luovuttamisen, säilytyksen, poistamisen, ulkoistamisen, poikkeamien eskaloinnin, rekisteröidyn oikeuksia koskevien pyyntöjen reitityksen, katselmoinnin ja todentavan aineiston hallinnan.

1.4 Tämä politiikka ei tarjoa työoikeudellista neuvontaa, henkilöstön edustuselimiä koskevaa oikeudellista kommentaaria, lainvalvontamenettelyä eikä erillistä kameravalvontarekisteriä. Valvontakohtainen todentava aineisto ylläpidetään tässä politiikassa yksilöidyissä kanonisissa PIMS-näyttöobjekteissa.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on määrittää tietosuojakontrollit kameravalvonnalle ja fyysiselle valvonnalle siten, että valvontatoimet ovat tarkoitussidonnaisia, läpinäkyviä, oikeasuhtaisia, pääsynhallittuja, määritettyjen määräaikojen mukaisesti säilytettäviä, vain hyväksyttyjen kanavien kautta luovutettavia ja auditoitavissa olevalla PIMS-todentavalla aineistolla tuettuja.

2.2 Tämä politiikka tukee valvontatallenteiden, vierailijatietojen, fyysisen pääsyn lokien ja niihin liittyvän valvonnassa käsiteltävän PII:n yhdenmukaista käsittelyä ilman lisärekisterien, komiteoiden, mittaristojen tai ei-kanonisten roolien luomista.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää valvonnan tarkoitukset ja käsittelyn soveltamisala ennen valvonnan aloittamista;

3.1.2 dokumentoida kameravalvonta, fyysinen pääsy, vierailijoiden valvonta ja fyysisen valvonnan toiminnot REG02:ssa;

3.1.3 tunnistaa valvontatoimet, jotka edellyttävät tietosuojariskin arviointia tai DPIA-esiarviointia REG04:ssä;

3.1.4 ylläpitää läpinäkyvää tietosuojaseloste- ja valvontakylttinäyttöä REG07:ssä;

3.1.5 rajoittaa valvontaan liittyvän PII:n pääsyä, katselua, vientiä, luovuttamista ja säilytystä;

3.1.6 reitittää rekisteröityjen pyynnöt REG06:n kautta;

3.1.7 hallita ulkoistettuja valvontapalveluntarjoajia ja tietojen jakamista koskevaa näyttöä REG08:ssa;

3.1.8 eskaloida epäillyt valvontaan liittyvät henkilötietopoikkeamat REG10:n kautta;

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

4. Politiikkalausekkeet

4.1 Valvonnan luettelo, tarkoitus ja hyväksyntä

4.1.1 [Controller] Process Owner / Business Owner TULEE kirjata jokainen kameravalvonta-, vierailijoiden valvonta-, fyysisen pääsynhallinnan loki- tai fyysisen valvonnan toiminto REG02:een ennen toiminnon aloittamista.

4.1.2 [Controller] Privacy Lead / PIMS Manager TULEE validoida REG02-kirjaus tarkoituksen, oikeusperusteen, valvottavan sijainnin, PII-luokkien, rekisteröityjen ryhmien, säilytyksen, tietosuojaselosteen, pääsyn ja luovutuskenttien osalta ennen uuden tai olennaisesti muutetun valvontatoiminnon aktivointia.

4.1.3 [Controller] Process Owner / Business Owner TULEE kirjata hyväksytyt valvottavat vyöhykkeet, poissuljetut vyöhykkeet ja keräämisen rajat REG02:een ennen kameroiden, antureiden, vierailijalokien tai pääsynhallinnan lokituksen käyttöönottoa.

4.1.4 [Conditional] Process Owner / Business Owner TULEE hankkia REG04:n tietosuojariskipäätös ennen sellaisen valvonnan aktivointia, joka sisältää järjestelmällistä valvontaa, äänitallennusta, biometristä tunnistamista, analytiikkaa hyödyntävää havaitsemista, arkaluonteisia sijainteja, haavoittuvassa asemassa olevia henkilöitä tai ei-ilmeistä valvontaa.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager TULEE kirjata yhteisen valvonnan vastuunjako REG08:aan ennen kuin jaettu valvonta vuokranantajan, toimitilakumppanin, asiakkaan tai muun yhteisrekisterinpitäjän kanssa alkaa.

4.1.6 [Processor] Privacy Lead / PIMS Manager TULEE kirjata asiakkaan valvontaa koskevat ohjeet ja sallitut käsittelyn rajat REG08:aan ennen valvontatallenteiden, vierailijatietojen tai fyysisen pääsyn lokien käsittelyä asiakkaan puolesta.

4.2 Tietosuojaselosteet ja läpinäkyvyys

4.2.1 [Controller] Process Owner / Business Owner TULEE varmistaa, että valvontakyltit tai vastaava oikea-aikainen ilmoitusnäyttö kirjataan REG07:ään ennen valvottujen alueiden avaamista rekisteröidyille.

4.2.2 [Controller] Privacy Lead / PIMS Manager TULEE liittää jokainen REG07:ssä oleva valvontaa koskeva tietosuojaseloste vastaavaan REG02:n käsittelytarkoitukseen ennen julkaisua tai olennaista muutosta.

4.2.3 [Processor] Privacy Lead / PIMS Manager TULEE toimittaa valvontaa koskevat tietosuojaselostetta tukevat tiedot REG08:ssa, kun organisaatio tuottaa valvontapalveluja asiakkaan ohjeiden mukaisesti.

4.2.4 [Conditional] Process Owner / Business Owner TULEE kirjata vaihtoehtoiset läpinäkyvyystoimet REG07:ään ja REG04:ään ennen ei-ilmeisen tai hätätilanteeseen liittyvän valvonnan aktivointia.

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

9. Poikkeukset

9.1 [All] Privacy Lead / PIMS Manager TULEE kirjata jokainen tätä politiikkaa koskeva poikkeus REG12:een ennen poikkeuksen käyttämistä.

9.2 [Conditional] Data Protection Officer / Privacy Advisor TULEE dokumentoida tietosuojaneuvonta REG04:ssä tai REG12:ssa ennen sellaisten poikkeusten hyväksymistä, jotka koskevat ei-ilmeistä valvontaa, äänitallennusta, biometristä tunnistamista, analytiikkaa hyödyntävää valvontaa tai arkaluonteisia valvontasijainteja.

9.3 [All] Top Management TULEE hyväksyä yli 90 päivää kestävät poikkeukset REG12:ssa ennen alkuperäisen poikkeusjakson ylittävää jatkoa.

9.4 [All] Privacy Lead / PIMS Manager TULEE katselmoida avoimet valvontaa koskevat poikkeukset REG12:ssa vähintään kuukausittain niiden sulkemiseen saakka.

10. Soveltaminen

10.1 [All] Privacy Lead / PIMS Manager TULEE kirjata valvontakontrollien epäonnistumiset poikkeamina REG12:een viiden työpäivän kuluessa vahvistamisesta.

10.2 [Both] Information Security Lead TULEE keskeyttää luvaton pääsy valvontajärjestelmään yhden työpäivän kuluessa vahvistamisesta ja kirjata toimi REG10:een tai REG12:een.

10.3 [All] Top Management TULEE nimetä korjaavan toimenpiteen omistajuus REG12:ssa 10 työpäivän kuluessa toistuvista tai olennaisista politiikan rikkomuksista.

10.4 [Conditional] Incident Response Coordinator TULEE käynnistää henkilötietopoikkeaman työnkulku REG10:ssä, kun epäillään valvontaan liittyvän PII:n luvatonta luovuttamista, katoamista tai vaarantumista.

11. Katselmointi ja ylläpito

11.1 [All] Privacy Lead / PIMS Manager TULEE katselmoida tämä politiikka ja siihen liittyvä valvontanäyttö REG12:ssa vähintään vuosittain.

11.2 [Controller] Process Owner / Business Owner TULEE uudelleenvalidoida jokainen aktiivinen valvonnan tarkoitus, tietosuojaseloste, sijainnin soveltamisala ja säilytyskirjaus REG02:ssa ja REG07:ssä vähintään vuosittain.

11.3 [Both] System Owner / Application Owner TULEE uudelleenvalidoida valvontajärjestelmän pääsy-, lokitus-, poisto- ja vientikontrollit REG12:ssa vähintään vuosittain ja olennaisen järjestelmämuutoksen jälkeen.

11.4 [Conditional] Vendor / Procurement Owner TULEE uudelleenvalidoida ulkoistettua valvontapalveluntarjoajaa koskeva näyttö REG08:ssa vähintään vuosittain ja ennen sopimuksen uusimista.

11.5 [All] Privacy Lead / PIMS Manager TULEE päivittää siihen liittyvä REG02-, REG04-, REG07-, REG08-, REG10- tai REG12-näyttö 30 kalenteripäivän kuluessa hyväksytyistä politiikkamuutoksista.

12. Liittyvät politiikat

12.1 PII02 - Tietosuojaroolien, vastuiden ja osoitusvelvollisuuden politiikka

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

12.3 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.4 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.5 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.6 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

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

12.8 PII10 - PII:n säilytys-, poisto- ja hävityspolitiikka

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

12.10 PII13 - PII:n kansainvälisten siirtojen politiikka

12.11 PII14 - PII:n tietoturva- ja pääsynhallintapolitiikka

12.12 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.13 PII17 - PIMS:n dokumentoidun tiedon ja todentavan aineiston hallintapolitiikka

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

12.15 PII19 - Työntekijöiden tietosuojapolitiikka

12.16 PII21 - Tekoälyn ja automaattisen päätöksenteon tietosuojapolitiikka

12.17 PII23 - Pilvipalvelujen PII-käsittelijäpolitiikka

13. Viitestandardit ja viitekehykset

13.1 Tämä politiikka on yhdistetty seuraaviin standardeihin ja säädöksiin. Vastaavuus kuvaa, miten politiikka tukee viitattuja vaatimuksia, ja tunnistaa sisäiset lausekkeet, joilla ne toteutetaan tai joita ne tukevat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Yhdistetty dokumentoituun valvontanäyttöön, operatiiviseen suunnitteluun, aktivointikontrolleihin, tarkoitustallenteisiin, tietosuojaselosteen linkitykseen, pääsyn konfigurointiin, säilytyksen konfigurointiin ja kameravalvonnan sekä fyysisen valvonnan toimintojen muutoksenhallintaan. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Yhdistetty valvontakontrollien mittaamiseen, palveluntarjoajan katselmointiin, käyttöoikeuskatselmointiin, auditointihavaintoihin, poikkeamiin, korjaaviin toimenpiteisiin, erääntyneiden toimien eskalointiin ja parantamisnäyttöön. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Yhdistetty rekisterinpitäjän valvonnan tarkoituksen määrittelyyn, oikeusperusteen dokumentointiin, tietosuojariskin herätepäätöksiin ja valvonnan käsittelytoimien tallenteisiin REG02:ssa ja REG04:ssä. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Yhdistetty ulkoistetun valvontapalveluntarjoajan vastuunjakoon, yhteisen valvonnan vastuunjakoon ja henkilötietojen käsittelijää tai yhteisrekisterinpitäjää koskevaan näyttöön REG08:ssa. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Yhdistetty valvontaan liittyviin rekisteröityä koskeviin velvoitteisiin, pyyntöjen reititykseen, pyyntöjen arvioimiseksi tarvittavaan säilyttämiseen ja oikeuksien tukemisen hallinnointinäyttöön. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **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** - Yhdistetty valvonnan keräämisen rajoittamiseen, käsittelyn rajoihin, minimointiin, säilytysaikoihin, poistamiseen, ylikirjoitukseen, säilytyksen pidätyksiin ja poimittujen kopioiden hallintaan. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Yhdistetty ulkoisten luovutusten tallenteisiin, luovutuspyyntöjen käsittelyyn, minimointiin ennen luovutusta ja valvontaan liittyvää PII:tä koskeviin poikkeamiin liittyviin luovutuksiin. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Yhdistetty henkilötietojen käsittelijän asiakkaan ohjeisiin, sallittuihin käsittelyn rajoihin, tietosuojaselosteen tukeen, säilytys- ja poisto-ohjeisiin, oikeuksia koskevaan avustamiseen ja ulkoistettujen valvontapalvelujen henkilötietojen käsittelijän tallenteisiin. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Yhdistetty henkilötietojen käsittelijän tukeen asiakkaan velvoitteille, luovutusvaltuutukseen, luovutustallenteisiin, luovutuspyyntöjä koskeviin ilmoituksiin ja oikeudellisesti sitovaan valvontaan liittyvän PII:n luovutusten käsittelyyn. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Yhdistetty valvontatallenteiden suojaamiseen, rajoitettuun pääsyyn, etuoikeutettujen käyttöoikeuksien katselmointiin, käytön lokitukseen, luvattoman pääsyn rajaamiseen ja valvontajärjestelmien lokitusnäyttöön. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Yhdistetty lainmukaisuuteen, kohtuullisuuteen, läpinäkyvyyteen, käyttötarkoitussidonnaisuuteen, tietojen minimointiin, säilytyksen rajoittamiseen ja valvontatoimintojen osoitusvelvollisuusnäyttöön. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Yhdistetty kameravalvonnan, vierailijoiden valvonnan, fyysisen pääsyn lokien ja muiden fyysisen valvonnan toimintojen oikeusperusteen dokumentointiin. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Yhdistetty läpinäkyviin valvontaa koskeviin tietosuojaselosteisiin, valvontakylttinäyttöön, tietosuojaselosteiden linkittämiseen käsittelytarkoituksiin, henkilötietojen käsittelijän tietosuojaselostetta tukeviin tietoihin ja vaihtoehtoisiin läpinäkyvyystoimiin. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Yhdistetty pääsyyn, oikaisuun, poistamiseen, rajoittamiseen, vastustamiseen, pyyntöjen reititykseen, pyyntöjen arvioimiseksi tarvittavaan säilyttämiseen ja valvontaan liittyvään asiakasavustukseen. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Yhdistetty rekisterinpitäjän hallinnointiin, yhteisrekisterinpitäjien vastuunjakoon, henkilötietojen käsittelijöiden hallinnointiin, käsittelytoimien tallenteisiin, valvontajärjestelmien turvallisuuteen, tietosuojariskien arviointiin, DPIA-herätteisiin ja tietosuojaneuvontaan. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Yhdistetty tarkoituksen määrittelyyn, keräämisen rajoittamiseen, tietojen minimointiin, käytön rajoittamiseen, säilytyksen rajoittamiseen ja valvontaan liittyvän PII:n luovutusten rajoittamiseen. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Yhdistetty läpinäkyvyyteen, yksilön osallistumiseen, osoitusvelvollisuuteen, tietoturvaan, vaatimustenmukaisuuden katselmointiin, käyttöoikeuskatselmointiin, oikeuksia koskevien pyyntöjen reititykseen, poikkeamien eskalointiin ja korjaavien toimenpiteiden näyttöön. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Yhdistetty tietosuojariskin ja DPIA-herätteiden seulontaan järjestelmällisen, ei-ilmeisen, ääntä käyttävän, biometrisen, analytiikkaa hyödyntävän, arkaluonteiseen sijaintiin liittyvän, haavoittuvassa asemassa oleviin henkilöihin kohdistuvan tai muun korkeamman riskin fyysisen valvonnan osalta. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Yhdistetty PII:n suojaamiskontrolleihin tarkoituksen, keräämisen, minimoinnin, säilytyksen, luovuttamisen ja rekisteröidyn osallistumisen osalta valvontayhteyksissä. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Yhdistetty käyttöoikeuksien myöntämiseen, tiedonsaannin rajoittamiseen ja fyysisen sisäänpääsyn hallintakeinoihin, jotka liittyvät valvontajärjestelmän pääsyyn ja fyysisen pääsynhallinnan tallenteisiin. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Yhdistetty PII:n tietosuojaan ja suojaamiseen, fyysiseen sisäänpääsyyn, fyysisen turvallisuuden valvontaan, etuoikeutettuun pääsyyn, tiedonsaannin rajoittamiseen sekä kameravalvonnan ja fyysisen valvonnan järjestelmien lokituskontrolleihin. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].