| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Lisää tähän rekisteröidyn oikeushenkilön nimi | | | | | | | |
| Asiakirjan numero:<br>PII19 | | | | | Asiakirjan nimi:<br>**Työntekijöiden tietosuojapolitiikka** | | | | | | | |
| Versio:<br>1.0 | | Voimaantulopäivä:<br>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

| Standard / Regulation | Clause / Control / Article | Applicability | Coverage Type | Comment |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.5; Clause 8.1 | Both | Primary | Työntekijöiden tietosuojan todentava aineisto ja operatiivinen kontrolli |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | 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.1.2.8; Annex A.1.2.9 | Controller | Primary | HR-tarkoitukset, oikeusperusteyhteys, DPIA-heräte, yhteinen vastuunjako ja tallenteet |
| ISO/IEC 27701:2025 | Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7 | Both | Supporting | HR-palvelujen henkilötietojen käsittelijöiden sopimukset, ohjeet, avustaminen ja tallenteet |
| ISO/IEC 27701:2025 | Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11 | Controller | Supporting | Työntekijöitä koskevat velvoitteet, oikeudet ja automaattisen päätöksenteon ohjaus |
| 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 ja säilytyksen yhteys |
| ISO/IEC 27701:2025 | Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6 | Both | Supporting | Luovutuskirjaukset ja oikeudellisesti sitovien luovutusten käsittely |
| ISO/IEC 27701:2025 | Annex A.3.14; Annex A.3.25 | Both | Supporting | HR-tallenteiden suojaus ja lokitusnäyttö |
| GDPR | Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2) | Controller | Primary | Työntekijöiden tietosuojaperiaatteet ja osoitusvelvollisuus |
| GDPR | Article 6; Article 9; Article 10 | Controller | Supporting | Lainmukaisuus, erityiset |

| | | | | |
|---|---|---|---|---|
| | | | | henkilötietoryhmät ja taustaselvitystiedot |
| GDPR | Article 12; Article 13; Article 14 | Controller | Primary | Työntekijöiden informointi ja tietosuojaselosteet |
| GDPR | Article 15; Article 16; Article 17; Article 18; Article 21; Article 22 | Controller | Supporting | Työntekijöiden oikeudet ja automaattisen päätöksenteon ohjaus |
| GDPR | Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39 | Both | Supporting | Hallinnointi, yhteisrekisterinpitäjät, 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, käyttö, säilytys ja luovutus |
| 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 29151:2022 | Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10 | Controller | Supporting | PII-tarkoitus, kerääminen, minimointi, säilytys ja rekisteröidyn osallistuminen |
| ISO/IEC 29151:2022 | Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2 | Controller | Supporting | Henkilötietoja suojaavat työvoiman elinkaaren kontrollit |
| ISO/IEC 29151:2022 | Clause 15.1.2; Clause 15.2.2; Clause 15.2.3 | Both | Supporting | HR-palvelujen henkilötietojen käsittelijöiden arviointi, seuranta ja muutoksenhallinta |
| ISO/IEC 29134:2020 | Clause 5.1; Clause 6.2 | Controller | Supporting | HR:n tietosuojariski ja DPIA-herätteen yhteys |
| ISO/IEC 27002:2022 | Controls 5.34; 6.1; 6.2; 6.5; 6.6 | Both | Supporting | PII:n suojaus sekä työvoiman tietoturvan elinkaaren hallinta |
| ISO/IEC 27002:2022 | Controls 8.15; 8.16 | Both | Supporting | Lokitus- ja seurantatoimet |

## 1. Soveltamisala

1.1 Tämä politiikka määrittää työntekijöiden tietosuojaa koskevat vaatimukset, jotka liittyvät työntekijöiden henkilötietojen keräämiseen, käyttöön, luovuttamiseen, säilytysyhteyteen, informointiin, oikeuksien käsittelyyn, valvontaan, henkilötietojen käsittelijöiden tukeen ja todentavan aineiston hallintaan henkilötietojen hallintajärjestelmässä.

1.2 Tässä politiikassa ”työntekijöiden henkilötiedot” sisältävät työntekijöihin, työnhakijoihin, entisiin työntekijöihin, sopimuskumppaneihin, määräaikaiseen henkilöstöön, harjoittelijoihin, komennettuihin työntekijöihin ja muihin työvoimaan kuuluviin henkilöihin liittyvät henkilötiedot, kun organisaatio käsittelee heidän henkilötietojaan työvoimaan, rekrytointiin, työsuhteeseen, sitouttamiseen, palkitsemiseen, etuuksiin, turvallisuuteen, vaatimustenmukaisuuteen, työpaikan hallinnointiin tai niihin liittyviin liiketoimintatarkoituksiin.

1.3 Tämä politiikka koskee rekisterinpitäjä- ja yhteisrekisterinpitäjätilanteita, joissa organisaatio määrittää työntekijöiden henkilötietojen käsittelyn tarkoitukset ja keinot.

1.4 Tämä politiikka koskee myös henkilötietojen käsittelijä- ja alikäsittelijätilanteita, joissa organisaatio käsittelee työntekijöiden henkilötietoja asiakkaan, ylemmän tason henkilötietojen käsittelijän tai muun rekisterinpitäjän lukuun dokumentoitujen ohjeiden mukaisesti.

**1.5 Tämä politiikka kattaa:**

1.5.1 työntekijätietojen keräämisen;

1.5.2 HR-käsittelyn tarkoitukset;

1.5.3 työntekijöiden tietosuojaselosteet;

1.5.4 työntekijöiden oikeuksien käsittelyn;

1.5.5 säilytysyhteyden;

1.5.6 työntekijöiden valvonnan;

1.5.7 sisäisen luovutuksen;

1.5.8 HR-palvelujen henkilötietojen käsittelijöiden, palkanlaskennan, HRIS:n, etuuksien, taustaselvitysten ja ulkoistettujen HR-palvelujen kontrollit soveltuvin osin;

1.5.9 työntekijöiden henkilötietopoikkeamat, poikkeamat, korjaavat toimenpiteet ja parantamisnäytön.

1.6 Tämä politiikka ei luo erillistä HR-tietosuojarekisteriä, työntekijöiden tietosuojarekisteriä, HR-käsittelyrekisteriä, työntekijöiden valvontarekisteriä, taustaselvitysrekisteriä, HR-toimittajarekisteriä, työntekijöiden oikeuksien rekisteriä tai työntekijäpoikkeamarekisteriä. Työntekijöiden käsittelyä koskeva näyttö kirjataan kohteisiin REG02, REG04, REG06, REG07, REG08, REG10 ja REG12.

1.7 Tämä politiikka ei anna työoikeudellista neuvontaa, työmarkkinasuhteita koskevaa neuvontaa, yritysneuvoston oikeudellista kommentointia, kurinpitomenettelyjen sisältöä, palkanlaskennan toimintaohjeiden sisältöä tai lainkäyttöaluekohtaisia työsuhdeasiakirjamalleja.

**1.8 Tämä politiikka ei toista:**

1.8.1 PIMS-hallinnointia kohdassa PII01;

1.8.2 roolien vastuita kohdassa PII02;

1.8.3 käsittelytoimien luetteloa ja oikeusperusteen omistajuutta kohdassa PII03;

1.8.4 tietosuojaselosteen sisällön hallinnointia kohdassa PII04;

1.8.5 suostumuksen ja valinta-asetusten toimintaa kohdassa PII05;

1.8.6 rekisteröidyn oikeuksien työnkulkua kohdassa PII06;

1.8.7 tietosuojariskien ja DPIA:n menetelmää kohdassa PII07;

1.8.8 sisäänrakennetun tietosuojan portteja kohdassa PII08;

1.8.9 PII:n keräämisen, käytön, luovuttamisen ja jakamisen perussääntöjä kohdassa PII09;

1.8.10 säilytyksen, poistamisen ja hävittämisen toteutusta kohdassa PII10;

1.8.11 oikeellisuuden ja laadun hallinnointia kohdassa PII11;

1.8.12 henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten elinkaaren hallinnointia kohdassa PII12;

1.8.13 henkilötietojen kansainvälisten siirtoperusteiden kontrolleja kohdassa PII13;

1.8.14 turvallisuuden ja pääsynhallinnan toteutusta kohdassa PII14;

1.8.15 poikkeamien ja tietoturvaloukkausten käsittelyä kohdassa PII15;

1.8.16 koulutuksen ja tietoisuuden hallintaa kohdassa PII16;

1.8.17 dokumentoidun tiedon hallintaa kohdassa PII17;

1.8.18 PIMS-seurannan, auditoinnin ja parantamisen hallinnointia kohdassa PII18;

1.8.19 tekoälyn ja automaattisen päätöksenteon kontrolleja kohdassa PII21, jos kyseinen valinnainen politiikka sisältyy kokonaisuuteen.

## 2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että työntekijöiden henkilötietoja käsitellään vain dokumentoituihin, hyväksyttyihin, läpinäkyviin, oikeasuhtaisiin ja osoitusvelvollisuuden mukaisiin työvoimaa koskeviin tarkoituksiin ja että työntekijöiden tietosuojan näyttö ylläpidetään kanonisissa PIMS-rekistereissä luomatta erillistä HR-tietosuojan näyttökerrosta.

2.2 Tämä politiikka tukee työntekijöiden käsittelyn yhdenmukaista hallintaa liittämällä työntekijöiden käsittelytoimet kohteeseen REG02, työntekijöiden tietosuojaselosteet kohteeseen REG07, työntekijöiden oikeuksia koskevat pyynnöt kohteeseen REG06, HR-tietosuojariskit ja DPIA-herätteet kohteeseen REG04, HR-palvelujen henkilötietojen käsittelijät sekä palkanlaskennan tai HRIS-toimittajat kohteeseen REG08, työntekijöiden henkilötietopoikkeamat kohteeseen REG10 sekä poikkeukset, poikkeamat, korjaavat toimenpiteet ja seurantanäytön kohteeseen REG12.

## 3. Tavoitteet

### 3.1 Tämän politiikan tavoitteena on:

3.1.1 ylläpitää työntekijöiden käsittelytoimien luetteloa koskeva näyttö kohteessa REG02;

3.1.2 dokumentoida työntekijöiden tietojen keräyslähteet, PII-luokat, tarkoitukset, järjestelmät, vastaanottajat ja säilytysyhteys;

3.1.3 ylläpitää työntekijöiden tietosuojaselosteita koskeva näyttö kohteessa REG07;

3.1.4 ohjata työntekijöiden tietosuojariskit ja DPIA-herätteet kohteen REG04 kautta;

3.1.5 ohjata työntekijöiden oikeuksia koskevat pyynnöt kohteen REG06 kautta;

3.1.6 ylläpitää HR-palvelujen henkilötietojen käsittelijöitä, palkanlaskentaa, HRIS:ää, etuuksia, taustaselvityksiä ja ulkoistettuja HR-palveluja koskeva näyttö kohteessa REG08;

3.1.7 varmistaa, että työntekijöiden valvonta on dokumentoitu, oikeasuhtaista, katselmoitu ja eskaloitu kohteiden REG04 ja REG12 kautta soveltuvin osin;

3.1.8 ohjata epäillyt työntekijöiden henkilötietopoikkeamat kohteen REG10 kautta;

3.1.9 kirjata työntekijöiden tietosuojaa koskevat poikkeukset, poikkeamat, korjaavat toimenpiteet ja parantamistoimet kohteeseen REG12;

3.1.10 välttää työoikeudellista neuvontaa ja yritysneuvostoa koskevaa oikeudellista kommentointia operatiivisissa kohdissa;

3.1.11 välttää päällekkäisiä rekistereitä, rooleja, lomakkeita, mittaristoja tai HR-kohtaisia näyttöobjekteja.

## 4. Politiikkalausekkeet

### 4.1 Työntekijöiden käsittelytoimien luettelo ja HR-käsittelyn tarkoitukset

4.1.1 [Controller] Process Owner / Business Owner tulee kirjata jokainen työntekijöiden käsittelytoimi kohteeseen REG02 ennen kuin työntekijöiden henkilötietoja kerätään, tuotetaan, tuodaan, käytetään tai luovutetaan.

4.1.2 [Controller] Process Owner / Business Owner tulee dokumentoida työntekijöiden PII-luokat, työntekijäjoukko, keräyslähde, käsittelyn tarkoitus, järjestelmä, sisäisen vastaanottajan luokka, ulkoisen vastaanottajan luokka ja säilytysyhteys kohteeseen REG02 ennen käsittelytoimen hyväksymistä.

4.1.3 [Controller] Privacy Lead / PIMS Manager tulee katselmoida jokainen uusi tai olennaisesti muuttunut työntekijöiden käsittelytoimi kohteessa REG02 ennen kuin käsittelytoimi hyväksytään käyttöön.

4.1.4 [Conditional] Data Protection Officer / Privacy Advisor tulee kirjata tietosuojaneuvonta kohteeseen REG04 ennen työntekijöiden käsittelyn hyväksyntää, kun käsittely sisältää erityisiin henkilötietoryhmiin kuuluvaa PII:tä, rikostuomioihin tai rikkomuksiin liittyviä tietoja, taustaselvityksiä, työterveystietoja, biometrisiä tietoja, sijaintitietoja, työntekijöiden valvontaa tai käsittelyä, joka voi olennaisesti vaikuttaa työntekijään.

4.1.5 [Processor] Privacy Lead / PIMS Manager tulee kirjata asiakkaan ohje, palvelun tarkoitus, asiakkaan työntekijöiden PII-luokat ja henkilötietojen käsittelijän roolia koskeva yhteys kohteeseen REG08 ennen asiakkaan työntekijöiden henkilötietojen käsittelyä ulkoistettuna HR-, palkanlaskenta-, etuus-, HRIS-, seulonta- tai työvoiman tukipalveluna.

4.1.6 [Joint Controller] Privacy Lead / PIMS Manager tulee kirjata työntekijöiden henkilötietojen käsittelyä koskeva yhteisrekisterinpitäjien vastuunjako kohteeseen REG08 ennen yhteisen työntekijöiden käsittelytoimen aloittamista.

### 4.2 Työntekijätietojen kerääminen ja työntekijöiden tietosuojaselosteet

4.2.1 [Controller] Process Owner / Business Owner tulee rajoittaa työntekijöiden henkilötietojen kerääminen kohteessa REG02 dokumentoituihin luokkiin ennen rekrytoinnin, perehdytyksen, työsuhteen hallinnoinnin, etuuksien hallinnoinnin, palkanlaskennan, seulonnan, valvonnan tai palvelussuhteen päättämisen yhteydessä tapahtuvan keräämisen aloittamista.

4.2.2 [Controller] Process Owner / Business Owner tulee kirjata kolmansilta osapuolilta kerättyjen työntekijöiden henkilötietojen lähde kohteeseen REG02 ennen kolmannen osapuolen keräyslähteen käyttämistä.

4.2.3 [Controller] Privacy Lead / PIMS Manager tulee ylläpitää työntekijöiden tietosuojaselostetta koskeva kirjaus kohteessa REG07 ennen kuin työntekijöiden henkilötietoja kerätään suoraan tai välillisesti uuteen tai olennaisesti muuttuneeseen tarkoitukseen.

4.2.4 [Controller] Process Owner / Business Owner tulee varmistaa, että kohteeseen REG07 kirjattu ajantasainen työntekijöiden tietosuojaseloste on saatavilla ennen rekrytointiin liittyvää keräämistä, perehdytykseen liittyvää keräämistä, valvonnan aktivointia, etuuksiin ilmoittautumista, taustaselvitystä tai olennaista työntekijöiden käsittelymuutosta.

4.2.5 [Conditional] Data Protection Officer / Privacy Advisor tulee katselmoida kohteessa REG07 oleva työntekijöiden tietosuojaselostetta koskeva kirjaus ennen julkaisemista, kun seloste kattaa työntekijöiden valvonnan, taustaselvityksen, erityisiin henkilötietoryhmiin kuuluvan PII:n, rikostuomioihin tai rikkomuksiin liittyvät tiedot, automaattisen päätöksenteon tai olennaisesti muuttuneen työntekijöiden käsittelytarkoituksen.

4.2.6 [Processor] Vendor / Procurement Owner tulee kirjata työntekijöille suunnattujen keräyskanavien vastuut kohteeseen REG08 ennen kuin henkilötietojen käsittelijän ylläpitämä HR-, palkanlaskenta-, HRIS-, etuus-, seulonta- tai ulkoistettu HR-palvelu kerää työntekijöiden henkilötietoja asiakkaan lukuun.

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

## 9. Poikkeukset

9.1.1 [All] Process Owner / Business Owner tulee kirjata poikkeuspyyntö kohteeseen REG12 ennen mistään tämän politiikan vaatimuksesta poikkeamista.

9.1.2 [Conditional] Data Protection Officer / Privacy Advisor tulee kirjata neuvonta kohteeseen REG12 ennen sellaisen poikkeuksen hyväksymistä, joka vaikuttaa työntekijöiden valvontaan, työntekijöiden oikeuksien käsittelyyn, taustaselvitykseen, erityisiin henkilötietoryhmiin kuuluvaan PII:hin, rikostuomioihin tai rikkomuksiin liittyviin tietoihin tai vaikutuksiltaan merkittävään työntekijöiden käsittelyyn.

9.1.3 [Conditional] Top Management tulee hyväksyä työntekijöiden tietosuojapoikkeukset kohteessa REG12 ennen aktivointia, kun poikkeus vaikuttaa korkean riskin työntekijöiden käsittelyyn, työntekijöiden valvontaan, ulkoiseen luovutukseen, henkilötietojen käsittelijään tukeutumiseen tai ratkaisemattomaan korjaavaan toimenpiteeseen.

9.1.4 [All] Privacy Lead / PIMS Manager tulee määrittää jokaiselle työntekijöiden tietosuojapoikkeukselle kohteessa REG12 päättymispäivä, joka on enintään 90 päivän päässä, ennen poikkeuksen aktivointia.

9.1.5 [All] Privacy Lead / PIMS Manager tulee katselmoida jokainen työntekijöiden tietosuojapoikkeus kohteessa REG12 viiden arkipäivän kuluessa ennen sen päättymistä.

9.1.6 [All] Privacy Lead / PIMS Manager tulee sulkea tai eskaloida jokainen päättynyt työntekijöiden tietosuojapoikkeus kohteessa REG12 viiden arkipäivän kuluessa päättymisen jälkeen.

## 10. Soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager tulee kirjata poikkeama kohteeseen REG12 viiden arkipäivän kuluessa, kun työntekijöiden henkilötietojen käsittelyltä puuttuu vaadittu näyttö kohteesta REG02, REG07, REG08, REG04 tai REG06.

10.1.2 [Conditional] Incident Response Coordinator tulee kirjata epäilty luvaton pääsy työntekijöiden henkilötietoihin, luovutus, menetys tai vaarantuminen kohteeseen REG10 yhden arkipäivän kuluessa havaitsemisesta.

10.1.3 [Controller] Privacy Lead / PIMS Manager tulee estää uuden työntekijöiden valvonnan hyväksyntä kohteessa REG12, kun vaadittu näyttö kohteesta REG02, REG04 tai REG07 puuttuu.

10.1.4 [Both] Vendor / Procurement Owner tulee keskeyttää uusi työntekijöiden henkilötietojen luovutus HR-toimittajalle kohteessa REG08, kun vaadittu henkilötietojen käsittelijää, alikäsittelijää, ohjetta tai avustamista koskeva näyttö puuttuu.

10.1.5 [All] Top Management tulee katselmoida toistuvat työntekijöiden tietosuojan poikkeamat kohteessa REG12, kun sama luokka esiintyy kaksi tai useampia kertoja liukuvan 12 kuukauden jakson aikana.

10.1.6 [All] Internal Audit / Compliance Reviewer tulee todentaa sulkemisnäyttö kohteessa REG12 ennen työntekijöiden tietosuojakäsittelyä, työntekijöiden tietosuojaselosteita, työntekijöiden valvontaa, työntekijöiden oikeuksia tai HR-toimittajia koskevien auditointihavaintojen sulkemista.

## 11. Katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka kohteessa REG12 vähintään vuosittain.

11.1.2 [Conditional] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka kohteessa REG12 30 päivän kuluessa olennaisesta muutoksesta työntekijöiden käsittelyssä,

työntekijöiden valvonnassa, HR-järjestelmissä, palkanlaskentajärjestelyissä, HRIS-palveluntarjoajissa, etuuspalveluntarjoajissa, taustaselvityspalveluntarjoajissa tai ulkoistetuissa HR-palveluissa.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor tulee katselmoida tähän politiikkaan ehdotetut olennaiset muutokset kohteessa REG12 ennen kuin Top Management hyväksyy ne.

11.1.4 [All] Top Management tulee hyväksyä tämän politiikan olennaiset muutokset kohteessa REG12 ennen julkaisua.

11.1.5 [All] Privacy Lead / PIMS Manager tulee päivittää REG02, REG07 tai REG08 15 arkipäivän kuluessa sen jälkeen, kun hyväksytty politiikkamuutos vaikuttaa työntekijöiden käsittelykirjauksiin, työntekijöiden tietosuojaselosteisiin tai HR-toimittajien näyttöön.

11.1.6 [All] Internal Audit / Compliance Reviewer tulee kirjata tämän politiikan katselmoinnin vaikuttavuushavainnot kohteeseen REG12 suunnitellun PIMS-sisäisen auditointisyklin aikana.

## 12. Liittyvät politiikat

12.1 Tätä politiikkaa tukevat seuraavat liittyvät politiikat:

12.2 PII01 - Henkilötietojen hallintajärjestelmän politiikka

12.3 PII02 - Tietosuojan rooleja, vastuita ja osoitusvelvollisuutta koskeva politiikka

12.4 PII03 - PII-käsittelytoimien luetteloa ja oikeusperustetta koskeva politiikka

12.5 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.6 PII05 - Suostumuksen ja valinta-asetusten hallintapolitiikka

12.7 PII06 - Rekisteröityjen oikeuksien hallintapolitiikka

12.8 PII07 - Tietosuojariskien arviointi- ja DPIA-politiikka

12.9 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

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

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

12.12 PII11 - PII:n oikeellisuus- ja laatupolitiikka

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

12.14 PII13 - PII:n kansainvälisten siirtojen politiikka

12.15 PII14 - PII:n turvallisuus- ja pääsynhallintapolitiikka

12.16 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

12.17 PII16 - Tietosuojakoulutus-, tietoisuus- ja pätevyyspolitiikka

12.18 PII17 - PIMS-dokumentoidun tiedon ja näytönhallinnan politiikka

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

12.20 PII21 - Tekoälyn ja automaattisen päätöksenteon tietosuojapolitiikka, jos se sisältyy valinnaisen lisäosan julkaisun soveltamisalaan

## 13. Viitestandardit ja viitekehykset

13.1 Tämä politiikka on yhdistetty 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

13.2.1 **Clause 7.5; Clause 8.1** - Yhdistetty työntekijöiden tietosuojan dokumentoituun näyttöön, operatiivisiin hyväksyntäportteihin, HR-palvelujen henkilötietojen käsittelijöiden kirjauksiin, työntekijöiden tietosuojaselosteisiin, valvontakirjauksiin, poikkeusten käsittelyyn ja

toteutusnäyttöön. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Yhdistetty työntekijöiden tietosuojan seurantaan, mittareihin, auditointinäyttöön, työntekijöiden valvonnan otantaan, poikkeamien käsittelyyn, korjaaviin toimenpiteisiin ja parantamiseen. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Yhdistetty työntekijöiden käsittelytarkoituksiin, oikeusperusteyhteyteen, tietosuojariskien ja DPIA:n ohjaukseen, yhteisrekisterinpitäjien vastuunjakoon sekä käsittelykirjauksiin kohteissa REG02 ja REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Yhdistetty HR-palvelujen henkilötietojen käsittelijöiden sopimuksiin, dokumentoituihin ohjeisiin, asiakkaan työntekijöiden henkilötietojen käsittelyyn, henkilötietojen käsittelijän avustamiseen ja käsittelijän kirjauksiin kohteessa REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Yhdistetty työntekijöiden oikeuksien käsittelyyn, monimutkaisia oikeuksia koskevaan neuvontaan sekä automaattisen päätöksenteon tai vaikutuksiltaan merkittävän käsittelyn ohjaukseen kohteiden REG06 ja REG04 kautta. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

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 työntekijöiden tietojen keräämisen rajoittamiseen, hyväksyttyyn sisäiseen käyttöön, minimointiin, säilytysyhteyteen ja säilytyspoikkeusten ohjaukseen. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Yhdistetty työntekijöiden henkilötietojen ulkoisiin luovutuksiin, tietojen jakamista koskeviin kirjauksiin, henkilötietojen käsittelijän luovutusvaltuutukseen ja luovutuksiin liittyvien poikkeamien ohjaukseen. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].

13.2.8 **Annex A.3.14; Annex A.3.25** - Yhdistetty työntekijöiden tietosuojakirjausten suojaamiseen, työntekijöiden valvontalokien näyttöön sekä työntekijöiden valvontatietojen epäiltyyn väärinkäyttöön tai vaarantumiseen. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

**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 työntekijöiden henkilötietojen lainmukaiseen, asianmukaiseen, läpinäkyvään, käyttötarkoitussidonnaiseen, minimoituun, säilytykseen kytkettyyn ja osoitusvelvollisuuden mukaiseen käsittelyyn. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Yhdistetty oikeusperusteyhteyteen, erityisiin henkilötietoryhmiin kuuluvien työntekijöiden henkilötietojen ohjaukseen, työterveyttä ja työsuhdetta koskevan arkaluonteisen PII:n ohjaukseen sekä rikostuomioihin tai rikkomuksiin tai taustaselvityksiin liittyvien tietojen ohjaukseen. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Yhdistetty työntekijöiden läpinäkyvyyteen, työntekijöiden tietosuojaselostekirjauksiin, suoran ja välillisen keräämisen informointiherätteisiin sekä valvontaa koskevaan informointinäyttöön. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Yhdistetty työntekijöiden oikeuksien ohjaukseen, pyyntönäyttöön, monimutkaisia pyyntöjä koskevaan neuvontaan ja automaattisen päätöksenteon ohjaukseen. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Yhdistetty rekisterinpitäjän hallinnointiin, yhteisrekisterinpitäjien vastuunjakoon, HR-palvelujen henkilötietojen käsittelijöiden hallinnointiin, käsittelykirjauksiin, turvalliseen käsittelyyn, DPIA-ohjaukseen ja tietosuojaneuvonnan osallistumiseen. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Yhdistetty työntekijöiden käsittelyn tarkoituksen määrittelyyn, keräämisen rajoittamiseen, minimointiin, käytön rajoittamiseen, säilytyksen rajoittamiseen ja luovutusten rajoittamiseen. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Yhdistetty läpinäkyvyyteen, työntekijöiden osallistumiseen, työntekijöiden oikeuksien tukemiseen, osoitusvelvollisuuteen, tietoturvaan ja tietosuojan vaatimustenmukaisuusnäyttöön. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Yhdistetty PII-käsittelyn tarkoituskirjauksiin, keräyskontrolleihin, minimointiin, säilytysyhteyteen, luovutusten rajoittamiseen sekä työntekijöiden osallistumisen tai pääsyn tukemiseen. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Yhdistetty PII:tä suojaaviin työvoiman elinkaaren kontrolleihin, jotka koskevat seulontaa, ehtoja, tietosuojaloukkauksen soveltamisyhteyttä sekä työsuhteen päättymisen tai muutoksen yhteydessä tehtävää säilytyksen katselmointia. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Yhdistetty HR-palvelujen henkilötietojen käsittelijöiden arviointiin, HR-palvelujen henkilötietojen käsittelijöiden seurantaan, HR-toimittajien katselmointiin ja palvelumuutosten näyttöön kohteessa REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

**13.6 ISO/IEC 29134:2020**

13.6.1 **Clause 5.1; Clause 6.2** - Yhdistetty tietosuojaa koskevan vaikutustenarvioinnin hyötyihin sekä HR-tietosuojariskin tai DPIA-herätteen määrittämiseen työntekijöiden valvonnassa ja vaikutuksiltaan merkittävässä HR-käsittelyssä ilman DPIA-menetelmän toistamista. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

**13.7 ISO/IEC 27002:2022**

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Yhdistetty PII:n suojaamiseen, seulontaan, työvoimaa koskeviin ehtoihin, työsuhdemuutoksen jälkeisiin vastuisiin ja luottamuksellisuusodotuksiin PII:tä tukevina työvoiman elinkaaren kontrolleina. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Yhdistetty työntekijöiden valvontalokeihin, seurantatoimiin, lokien käyttötarkoituksen rajoittamiseen ja valvontanäytön katselmointiin. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].