					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII03					Asiakirjan nimi: **PII:n käsittelytoimien luetteloa ja oikeusperustetta koskeva politiikka**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	PIMS-roolin määrittäminen käsittelytoimille
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Tietosuojariskien arvioinnin käynnistämiseen liittyvä yhteys
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Kontrollien soveltuvuuden ja SoA:n yhteys
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Käsittelytoimien luettelon dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Käsittelytoimien tallenteiden operatiivinen suunnittelu ja ohjaus
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Operatiivisen tietosuojariskien arvioinnin yhteys
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Käsittelytoimien luettelon seuranta ja mittaaminen
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Käsittelytoimien luetteloon liittyvä poikkeama ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Rekisterinpitäjän tarkoituksen tunnistaminen
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Rekisterinpitäjän oikeusperusteen tunnistaminen
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	DPIA-tarpeen seulonnan yhteys
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Yhteisrekisterinpitäjien käsittelyvastuita koskevat tallenteet
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Rekisterinpitäjän PII:n käsittelyyn liittyvät tallenteet
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Henkilötietojen käsittelijän asiakassopimus- ja ohjetallenteet
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Henkilötietojen käsittelijän tarkoituksen yhdenmukaisuus asiakkaan ohjeiden kanssa

ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Henkilötietojen käsittelijän PII:n käsittelyyn liittyvät tallenteet
GDPR	Article 5(1)(a)	Controller	Supporting	Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden yhteys
GDPR	Article 5(1)(b)	Controller	Supporting	Käyttötarkoitussidonnaisuus
GDPR	Article 5(1)(c)	Controller	Supporting	Tietojen minimointi
GDPR	Article 5(1)(e)	Controller	Supporting	Säilytyksen rajoittamiseen liittyvä yhteys
GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuuden näyttö
GDPR	Article 6	Controller	Primary	Käsittelyn lainmukaisuus
GDPR	Article 9	Conditional	Supporting	Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyn edellytys
GDPR	Article 10	Conditional	Supporting	Rikostuomioita ja rikkomuksia koskevien tietojen käsittelyn edellytys
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän vastuu ja toimenpiteet
GDPR	Article 26	Joint Controller	Supporting	Yhteisrekisterinpitäjien järjestelyä koskevat tallenteet
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijän ohje- ja sopimustallenteet
GDPR	Article 30	Both	Primary	Käsittelytoimien selosteet
GDPR	Article 35	Controller	Supporting	DPIA-tarpeen seulonnan yhteys
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Tarkoituksen oikeutus ja määrittely
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Keräämisen rajoittaminen
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Tietojen minimointi
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Käytön, säilytyksen ja luovuttamisen rajoittaminen
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Osoitusvelvollisuus
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	PII:n suojausta koskevat kontrollit tarkoituksen oikeutukselle, keräämiselle, minimoinnille, käytölle,

				säilytykselle ja luovuttamiselle
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	PIA:n hyödyn ja käynnistämisen yhteys

1. Soveltamisala

1.1 Tässä politiikassa määritetään vaatimukset PII:n käsittelytoimien luettelon / ROPA:n ylläpitämiselle sekä oikeusperusteen, käsittelytarkoitusten, käsittelyroolien, PII-luokkien, rekisteröityjen ryhmien, vastaanottajien, säilytysviitteiden, siirtoviitteiden, henkilötietojen käsittelijän ohjeiden, yhteisrekisterinpitäjien tallenteiden ja tietosuojariskien seulontaan liittyvien yhteyksien dokumentoinnille.

1.2 Tätä politiikkaa sovelletaan:

1.2.1 kaikkiin PIMS:n soveltamisalaan kuuluviin PII:n käsittelytoimiin;

1.2.2 käsittelyyn, jota tehdään rekisterinpitäjänä, yhteisrekisterinpitäjänä, henkilötietojen käsittelijänä tai alikäsittelijänä;

1.2.3 käsittelyyn, jota suorittavat liiketoimintaprosessit, järjestelmät, sovellukset, toimittajat, henkilötietojen käsittelijät, alikäsittelijät ja tietojen jakamisen vastaanottajat;

1.2.4 uuteen käsittelyyn, olennaisesti muuttuneeseen käsittelyyn ja lopetettuun käsittelyyn;

1.2.5 REG02:ssa ylläpidettävään todentavaan aineistoon sekä sitä tukevaan todentavaan aineistoon REG01:ssä, REG03:ssa, REG04:ssä, REG05:ssä, REG07:ssä, REG08:ssa, REG09:ssä ja REG12:ssa.

1.3 Tämä politiikka ei korvaa yksityiskohtaisia tietosuojaselosteiden kontrolleja, suostumuskontrolleja, DPIA-menetelmää, säilytyksen toteutusta, kansainvälisen siirtomekanismin valintaa, henkilötietojen käsittelijöitä koskevia sopimuskontrolleja, PII:n turvallisuuskontrolleja eikä dokumentoidun tiedon kontrolleja. Nämä vaatimukset määritetään kohdassa 12 luetelluissa liittyvissä politiikoissa.

1.4 Tässä politiikassa käsittelytoimien luettelon tietue tarkoittaa REG02-merkintää, jossa kuvataan erillinen PII:n käsittelytoimi, mukaan lukien sen tarkoitus, rooli, omistaja, PII-luokat, rekisteröityjen ryhmät, oikeusperuste tai asiakkaan ohjeen viite, järjestelmät, vastaanottajat, säilytysviite, siirtoviite, tietosuojariskin tila ja katselmointitila.

1.5 Tässä politiikassa olennainen käsittelymuutos tarkoittaa mitä tahansa muutosta käsittelytarkoitukseen, oikeusperusteeseen, PIMS-rooliin, PII-luokkaan, rekisteröityjen ryhmään, vastaanottajaan, järjestelmään, toimittajaan, alikäsittelijään, käsittelypaikkaan, siirtoon, säilytyssääntöön, turvallisuusluokitukseen, tietosuojaselosteeseen, suostumusriippuvuuteen, DPIA-tilaan, asiakkaan ohjeeseen tai sertifioinnin soveltamisalaan.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että organisaatio voi tunnistaa, dokumentoida, perustella, katselmoida ja osoittaa PIMS:n soveltamisalaan kuuluvat PII:n käsittelytoimet.

2.2 Tämä politiikka mahdollistaa sen, että organisaatio ylläpitää kattavaa, ajantasaista ja auditointivalmista PII:n käsittelytoimien luetteloa, joka tukee lainmukaista käsittelyä, osoitusvelvollisuutta, tietosuojaselosteita, suostumusten hallintaa, tietosuojariskien arviointia, DPIA-tarpeen seulontaa, säilytystä, siirtojen hallinnointia, henkilötietojen käsittelijöiden hallinnointia ja PIMS-seurantaa.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 vahvistaa REG02 viralliseksi PII:n käsittelytoimien luettelon ja ROPA:n todentavan aineiston kohteeksi;

3.1.2 varmistaa, että jokaisella PII:n käsittelytoimella on vastuullinen omistaja;

3.1.3 erottaa toisistaan rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän käsittelytallenteet;

3.1.4 dokumentoida täsmälliset käsittelytarkoitukset ennen käsittelyn aloittamista;

3.1.5 dokumentoida oikeusperuste rekisterinpitäjän käsittelylle ennen käsittelyn aloittamista;

3.1.6 dokumentoida asiakkaan ohjeet henkilötietojen käsittelijän ja alikäsittelijän käsittelylle ennen käsittelyn aloittamista;

3.1.7 dokumentoida PII-luokat, rekisteröityjen ryhmät, vastaanottajat, säilytysviitteet, siirtoviitteet, järjestelmät ja toimittajasuhteet;

3.1.8 yhdistää käsittelytoimien luettelon tietueet tietosuojaselosteita, suostumusta, DPIA:ta, riskejä, toimittajia, siirtoja, kontrolleja ja auditointia koskevaan todentavaan aineistoon soveltuvin osin;

3.1.9 varmistaa, että käsittelytoimien luettelon tietueet katselmoidaan, päivitetään ja korjataan käsittelyn muuttuessa;

3.1.10 välttää erillisten oikeusperuste- tai käsittelytoimien luettelorekisterien luomista REG02:n ulkopuolelle.

4. Politiikkalausumat

4.1 Käsittelytoimien luettelon perustaso

4.1.1 [Both] Process Owner / Business Owner MUST luoda REG02-käsittelytoimien luettelon tietue ennen uuden PII:n käsittelytoimen aloittamista.

4.1.2 [Both] Process Owner / Business Owner MUST kirjata vaaditut REG02-kentät jokaisesta käsittelytoimesta ennen toiminnan aloittamista.

4.1.3 [Both] Privacy Lead / PIMS Manager MUST hyväksyä vaadittu REG02-kenttäkokonaisuus REG12:ssa ennen PIMS:n alkuperäistä käyttöönottoa ja sen jälkeen vuosittain.

4.1.4 [Both] Process Owner / Business Owner MUST luokitella organisaation PIMS-rooli kullekin käsittelytoimelle REG02:ssa ennen toiminnan aloittamista.

4.1.5 [Both] System Owner / Application Owner MUST yhdistää jokainen PII:tä käsittelevä järjestelmä tai sovellus asiaankuuluvaan REG02-käsittelytoimeen ennen järjestelmän tuotantokäyttöönottoa.

4.1.6 [Both] Vendor / Procurement Owner MUST yhdistää jokainen henkilötietojen käsittelijää, alikäsittelijää, kolmannen osapuolen kanssa jakamista tai yhteisrekisterinpitäjyyttä koskeva suhde REG08:ssa asiaankuuluvaan REG02-käsittelytoimeen ennen sopimuksen hyväksymistä tai käyttöönottoa.

4.2 Rekisterinpitäjän tarkoitusta ja oikeusperustetta koskevat tallenteet

4.2.1 [Controller] Process Owner / Business Owner MUST dokumentoida täsmällinen käsittelytarkoitus REG02:ssa ennen kuin PII:tä kerätään, käytetään, luovutetaan tai muutoin käsitellään.

4.2.2 [Controller] Privacy Lead / PIMS Manager MUST validoida REG02:ssa kirjattu oikeusperuste ennen rekisterinpitäjän käsittelyn aloittamista ja ennen kuin tarkoituksen muutos tulee voimaan.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor MUST kirjata neuvonsa REG12:ssa ennen uuden oikeusperusteen hyväksymistä korkean riskin käsittelylle, erityisiin henkilötietoryhmiin kuuluvalle PII:lle, rikostuomioita tai rikkomuksia koskeville tiedoille tai olennaisesti muuttuneelle rekisterinpitäjän käsittelylle.

4.2.4 [Controller] Process Owner / Business Owner MUST yhdistää REG02 REG05:een ennen kuin rekisterinpitäjän käsittely perustuu suostumukseen oikeusperusteena.

4.2.5 [Controller] Process Owner / Business Owner MUST kirjata oikeutettua etua koskevan arvioinnin viite REG04:ään ennen kuin rekisterinpitäjän käsittely perustuu oikeutettuihin etuihin.

4.2.6 [Conditional] Process Owner / Business Owner MUST kirjata erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyn edellytys REG02:ssa ennen erityisiin henkilötietoryhmiin kuuluvan PII:n käsittelyä.

4.2.7 [Conditional] Privacy Lead / PIMS Manager MUST kirjata rikostuomioita tai rikkomuksia koskevien tietojen käsittelyn valtuutusperuste REG02:ssa ennen rikostuomioita tai rikkomuksia koskevien tietojen käsittelyä.

4.2.8 [Controller] Process Owner / Business Owner MUST dokumentoida tarkoituksen yhteensopivuus ja tietosuojariskin seulonta REG02:ssa ja REG04:ssä ennen PII:n käyttämistä uuteen tarkoitukseen, jota ei ole aiemmin kirjattu.

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

9. Poikkeukset

9.1 Käsittelytoimien luettelon ja oikeusperusteen poikkeukset

9.1.1 [All] Process Owner / Business Owner MUST pyytää poikkeusta REG12:ssa ennen PII:n käsittelytoimen käyttämistä ilman vaadittua REG02-kenttää, oikeusperustetietuetta, asiakkaan ohjeen viitettä tai katselmointitilaa.

9.1.2 [All] Privacy Lead / PIMS Manager MUST arvioida kunkin käsittelytoimien luettelon poikkeuksen vaikutukset tietosuojaan, sertifiointiin ja toimintaan REG12:ssa 10 työpäivän kuluessa pyynnöstä.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUST kirjata neuvonsa REG12:ssa ennen sellaisen poikkeuksen hyväksymistä, joka koskee oikeusperustetta, erityisiin henkilötietoryhmiin kuuluvaa PII:tä, rikostuomioita tai rikkomuksia koskevia tietoja, korkean riskin käsittelyä, kansainvälisen siirron yhteyttä tai asiakkaan ohjeen rajoitusta.

9.1.4 [All] Top Management MUST hyväksyä yli 30 päivää kestävät, korkean riskin käsittelyyn vaikuttavat tai sertifioinnin soveltamisalaan vaikuttavat käsittelytoimien luettelon poikkeukset REG12:ssa ennen poikkeuksen voimaantuloa.

9.1.5 [All] Privacy Lead / PIMS Manager MUST asettaa kullekin hyväksytylle käsittelytoimien luettelon poikkeukselle enintään 90 päivän päättymispäivä REG12:ssa ennen hyväksyntää.

9.1.6 [All] Process Owner / Business Owner MUST sulkea tai arvioida uudelleen kukin käsittelytoimien luettelon poikkeus REG12:ssa viiden työpäivän kuluessa sen päättymisestä.

10. Soveltaminen

10.1 Käsittelytoimien luettelon ja oikeusperusteen soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager MUST kirjata puuttuva, virheellinen, vanhentunut tai hyväksymätön REG02-käsittelytoimien luettelon todentava aineisto poikkeamana REG12:ssa viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [Controller] Process Owner / Business Owner MUST keskeyttää uusi rekisterinpitäjän käsittely, jos vaadittu tarkoitusta tai oikeusperustetta koskeva todentava aineisto puuttuu REG02:sta ennen käynnistystä.

10.1.3 [Processor] Process Owner / Business Owner MUST keskeyttää uusi henkilötietojen käsittelijän käsittely, jos vaadittu asiakkaan ohjetta koskeva todentava aineisto puuttuu REG02:sta tai REG08:sta ennen palvelun käyttöönottoa.

10.1.4 [Both] System Owner / Application Owner MUST estää järjestelmän tuotantokäyttöönotto PII:n käsittelyä varten, jos vaadittu REG02-luettelon yhteys puuttuu ennen tuotantokäyttöönoton hyväksyntää.

10.1.5 [Both] Vendor / Procurement Owner MUST estää toimittajan, henkilötietojen käsittelijän, alikäsittelijän, kolmannen osapuolen vastaanottajan tai yhteisrekisterinpitäjän käyttöönotto, jos

vaadittu REG02:n ja REG08:n yhteyttä koskeva todentava aineisto puuttuu ennen sopimuksen hyväksyntää.

10.1.6 [All] Top Management MUST katselmoida ratkaisemattomat merkittävät käsittelytoimien luettelon tai oikeusperusteen poikkeamat REG12:ssa johdon katselmoinnin aikana.

10.1.7 [All] Internal Audit / Compliance Reviewer MUST varmistaa käsittelytoimien luettelon poikkeamia koskevien korjaavien toimenpiteiden vaikuttavuus REG12:ssa seuraavassa suunnitellussa auditoinnissa tai 60 päivän kuluessa sulkemisesta sen mukaan, kumpi tapahtuu ensin.

11. Katselmointi ja ylläpito

11.1 Politiikan katselmointi ja ylläpito

11.1.1 [All] Privacy Lead / PIMS Manager MUST katselmoida tämä politiikka REG12:ssa vuosittain ja 30 päivän kuluessa olennaisesta muutoksesta käsittelytoimien luetteloon, oikeusperusteeseen, henkilötietojen käsittelijän ohjeeseen, ROPA:an tai sertifiointivaatimuksiin.

11.1.2 [All] Privacy Lead / PIMS Manager MUST katselmoida REG02:n vähimmäiskenttävaatimukset REG12:ssa vuosittain ja 30 päivän kuluessa olennaisesta oikeudellisesta, sääntelyyn liittyvästä, sopimusperusteisesta tai käsittelyä koskevasta muutoksesta.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST katselmoida tätä politiikkaa koskevat tietosuojan kannalta merkittävät muutokset REG12:ssa ennen hyväksyntää.

11.1.4 [All] Top Management MUST hyväksyä tämän politiikan olennaiset muutokset REG12:ssa ennen julkaisemista.

11.1.5 [All] Privacy Lead / PIMS Manager MUST päivittää REG03 ja REG04 15 työpäivän kuluessa hyväksytyistä politiikkamuutoksista, jotka muuttavat kontrollien soveltuvuutta tai tietosuojariskien seulontavaatimuksia.

11.1.6 [All] Privacy Lead / PIMS Manager MUST kirjata tähän politiikkaan hyväksytyistä muutoksista viestiminen REG11:een 30 päivän kuluessa julkaisemisesta.

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 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.5 PII05 - Suostumusten ja valintojen 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 säilytys-, poisto- ja hävityspolitiikka

12.10 PII11 - PII:n oikeellisuus- ja laatupolitiikka

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

12.12 PII13 - Kansainvälisiä PII-siirtoja koskeva politiikka

12.13 PII14 - PII:n turvallisuus- ja pääsynhallintapolitiikka

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

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

13. Viitestandardit ja viitekehykset

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Yhdistetty organisaation PIMS-roolin määrittämiseen kullekin käsittelytoimelle sekä rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän kontekstien erottamiseen. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Yhdistetty tietosuojariskien arvioinnin käynnistämiseen liittyvään yhteyteen uusille ja olennaisesti muuttuneille PII:n käsittelytoimille. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Yhdistetty käsittelytoimien liittämiseen kontrollien soveltuvuuteen ja PIMS:n soveltuvuuslausunnon todentavaan aineistoon. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Yhdistetty käsittelytoimien luettelon, oikeusperusteen, henkilötietojen käsittelijän ohjeiden, katselmointien, poikkeusten ja korjaavien toimenpiteiden tallenteiden ylläpitämiseen hallittuna dokumentoituna tietona. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].

13.2.5 **Clause 8.1** - Yhdistetty operatiiviseen suunnitteluun ja ohjaukseen, joiden avulla käsittelytoimien luettelon tietueet luodaan, validoidaan, päivitetään, katselmoidaan ja päätetään ennen käsittelyn aloittamista tai muuttamista. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].

13.2.6 **Clause 8.2** - Yhdistetty operatiivisen tietosuojariskien arvioinnin yhteyteen käsittelytoimien luettelon tietueista sekä olennaisen käsittelymuutoksen käynnistäjiin. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Yhdistetty käsittelytoimien luettelon kattavuuden, oikeusperusteen validoinnin, ohjeyhteyden, katselmointitilan, DPIA-seulonnan yhteyden ja täsmäytyspoikkeusten seurantaan ja mittaamiseen. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.8 **Clause 10.2** - Yhdistetty käsittelytoimien luettelon ja oikeusperusteen poikkeamien, poikkeusten, korjaavien toimenpiteiden, soveltamisen ja vaikuttavuuden varmistamisen käsittelyyn. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

13.2.9 **Annex A.1.2.2** - Yhdistetty rekisterinpitäjän käsittelytarkoitusten tunnistamiseen ja dokumentointiin ennen PII:n keräämistä, käyttöä, luovuttamista tai muuta käsittelyä. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Yhdistetty rekisterinpitäjän käsittelyn oikeusperusteen määrittämiseen, dokumentointiin, validointiin ja osoittamiseen. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].

13.2.11 **Annex A.1.2.6** - Yhdistetty uusien ja olennaisesti muuttuneiden rekisterinpitäjän käsittelytoimien seulontaan DPIA-tarpeen arvioimiseksi. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Yhdistetty yhteisrekisterinpitäjien käsittelytarkoitusten ja vastuunjaon viitteiden kirjaamiseen. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Yhdistetty rekisterinpitäjän PII:n käsittelyyn liittyvien tallenteiden ylläpitämiseen, mukaan lukien tarkoitukset, luokat, vastaanottajat, säilytysviitteet, siirrot, oikeusperuste, riskien seulonta, omistaja, tila ja katselmointia koskeva todentava aineisto. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].

13.2.14 **Annex A.2.2.2** - Yhdistetty henkilötietojen käsittelijän asiakassopimukseen ja dokumentoitujen ohjeiden todentavaan aineistoon, mukaan lukien käsittelyn kohde, kesto, tarkoitus, PII-luokat ja rekisteröityjen ryhmät. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].

13.2.15 **Annex A.2.2.3** - Yhdistetty sen varmistamiseen, että henkilötietojen käsittelijän käsittelytarkoitukset pysyvät dokumentoitujen asiakkaan ohjeiden mukaisina. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].

13.2.16 **Annex A.2.2.7** - Yhdistetty henkilötietojen käsittelijän tallenteiden ylläpitämiseen PII:n käsittelystä asiakkaiden puolesta. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(a)** - Yhdistetty rekisterinpitäjän käsittelytarkoitukseen, oikeusperusteen validointiin ja osoitusvelvollisuuden todentavaan aineistoon ennen käsittelyn aloittamista. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].

13.3.2 **Article 5(1)(b)** - Yhdistetty tarkoituksen määrittelyyn, tarkoituksen yhteensopivuuden arviointiin ja dokumentoimattoman uuteen tarkoitukseen perustuvan käsittelyn estämiseen. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].

13.3.3 **Article 5(1)(c)** - Yhdistetty PII-luokkien, rekisteröityjen ryhmien ja lähdetietojen kirjaamiseen ennen käsittelyä minimoinnin arvioinnin tukemiseksi. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.3.4 **Article 5(1)(e)** - Yhdistetty säilytyssäännön tai säilytysviitteen kirjaamiseen kullekin käsittelytoimelle. Addressed by clauses [4.4.4; 8.1.6].

13.3.5 **Article 5(2)** - Yhdistetty käsittelytoimien luettelon, oikeusperusteen validoinnin, katselmoinnin, täsmäytyksen, auditointiotannan ja korjaavien toimenpiteiden osoitusvelvollisuuden todentavaan aineistoon. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].

13.3.6 Article 6 - Yhdistetty rekisterinpitäjän käsittelyn oikeusperusteen dokumentointiin ja validointiin, mukaan lukien suostumusyhteys, oikeutettua etua koskevan arvioinnin viite ja tarkoituksen yhteensopivuus. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].

13.3.7 Article 9 - Yhdistetty erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyn edellytyksen ja tietosuojaa koskevan neuvonnan kirjaamiseen ennen erityisiin henkilötietoryhmiin kuuluvan PII:n käsittelyä. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

13.3.8 **Article 10** - Yhdistetty rikostuomioita tai rikkomuksia koskevien tietojen valtuutusperusteen kirjaamiseen ennen käsittelyä. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].

13.3.9 **Article 24** - Yhdistetty rekisterinpitäjän hallinnointiin, katselmointiin, osoitusvelvollisuuteen ja johdon valvontaan käsittelytoimien luettelon ja oikeusperustetallenteiden osalta. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].

13.3.10 **Article 26** - Yhdistetty yhteisrekisterinpitäjän käsittelytarkoitukseen ja vastuunjaon todentavaan aineistoon. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.3.11 **Article 28** - Yhdistetty henkilötietojen käsittelijän ja alikäsittelijän ohjeisiin, sopimukseen, suhdeyhteyteen ja käyttöönoton kontrolleihin. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].

13.3.12 **Article 30** - Yhdistetty rekisterinpitäjän ja henkilötietojen käsittelijän käsittelytoimien selosteisiin, mukaan lukien käsittelytarkoitukset, PII-luokat, rekisteröityjen ryhmät, vastaanottajat, siirrot, säilytysviitteet ja asiakkaan ohjetallenteet. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].

13.3.13 **Article 35** - Yhdistetty DPIA-tarpeen seulontaan uusille, olennaisesti muuttuneille tai korkean riskin rekisterinpitäjän käsittelytoimille. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3** - Yhdistetty tarkoituksen oikeutukseen, tarkoituksen määrittelyyn, oikeusperusteyhteyteen ja tarkoituksen yhteensopivuutta koskevaan todentavaan aineistoon. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Yhdistetty keräämisen rajoittamiseen dokumentoimalla PII-luokat, rekisteröityjen ryhmät, lähteet ja perustelut ennen käsittelyn aloittamista. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Yhdistetty tietojen minimointiin luettelokenttävaatimusten, luokkien dokumentoinnin, vastaanottajien dokumentoinnin ja nykyisten käsittelytallenteiden katselmoinnin kautta. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Yhdistetty käytön, säilytyksen, luovuttamisen ja siirron rajoittamiseen dokumentoitujen tarkoitusten, vastaanottajaryhmien, säilytysviitteiden, siirtoyhteyksien ja tarkoituksen muutoksen kontrollien avulla. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Yhdistetty osoitusvelvollisuuteen omistajuuden, käsittelytoimien luettelon hallinnoinnin, katselmoinnin, täsmäytyksen, auditointiotannan, poikkeusten käsittelyn ja korjaavien toimenpiteiden todentavan aineiston kautta. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Yhdistetty PII:n suojauksen kontrolleihin, jotka koskevat tarkoituksen oikeutusta, keräämisen rajoittamista, tietojen minimointia sekä käytön, säilytyksen ja luovuttamisen rajoittamista. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Yhdistetty käsittelytoimien luettelon muutosten käyttämiseen tietosuojariskien arvioinnin ja DPIA-tarpeen seulonnan käynnistäjänä ennen uuden tai olennaisesti muuttuneen käsittelyn etenemistä. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].