					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII07					Asiakirjan nimi: **Tietosuojariskien arviointi- ja DPIA-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

Standardi / säädös	Lauseke / hallintakeino / artikla	Sovellettavuus	Kattavuustyyppi	Kommentti
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-riskit ja mahdollisuudet
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Tietosuojariskien arviointi
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tietosuojariskien käsittely ja yhteys SoA:han
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Suunnitellut PIMS-muutokset ja riskien uudelleenarviointi
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Tietosuojariskejä ja DPIA:ta koskeva dokumentoitu tieto
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operatiivinen suunnittelu ja ohjaus
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operatiivinen tietosuojariskien arviointi
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operatiivinen tietosuojariskien käsittely
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Tietosuojariskien seuranta ja mittaaminen
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Tietosuojariskien johdon katselmointi
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Riskeihin liittyvät poikkeamat ja korjaavat toimenpiteet
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Tietosuojaa koskeva vaikutustenarviointi
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Riskien arviointia tukevat käsittelytoimien tallenteet
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Henkilötietojen käsittelijän asiakassopimus ja vaikutustenarvioinnissa avustaminen
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Henkilötietojen käsittelijän tiedot asiakkaan vaatimustenmukaisuuden tueksi

GDPR	Article 5(2)	Controller	Supporting	Osoitusvelvollisuuden todentava aineisto
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän vastuu ja toimenpiteet
GDPR	Article 25	Controller	Supporting	Sisäänrakennettu ja oletusarvoinen tietosuoja
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijän avustaminen ja ohjeet
GDPR	Article 30	Both	Supporting	DPIA:ta tukevat käsittelytoimien tallenteet
GDPR	Article 32	Both	Supporting	Tietoturvariski ja suojatoimet
GDPR	Article 35	Controller	Primary	Tietosuojaa koskeva vaikutustenarviointi
GDPR	Article 36	Controller	Primary	Ennakkokuuleminen
GDPR	Article 39	Conditional	Supporting	DPO-neuvonta ja seuranta soveltuvin osin
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Tietosuojakontrollit, tietoturva ja tietosuojavaatimusten noudattaminen
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA:n soveltamisala, hyödyt, käynnistysperuste ja valmistelu
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII:n suojausohjelma ja vaatimusten tunnistaminen
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Organisaation tietosuojariskien hallinnan integrointi

1. Soveltamisala

1.1 Tämä politiikka määrittää vaatimukset tietosuojariskien arvioinnille, DPIA-esiarvioinnille, täysimittaisen DPIA:n toteuttamiselle, tietosuojariskien käsittelylle, jäännösriskin hyväksynnälle, kuulemiselle, katselmoinnille ja todentavan aineiston hallinnalle PIMS:n soveltamisalaan kuuluvassa PII:n käsittelyssä.

1.2 Tätä politiikkaa sovelletaan seuraaviin:

1.2.1 uudet ja olennaisesti muuttuneet PII:n käsittelytoimet;

1.2.2 rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän käsittelykontekstit;

1.2.3 järjestelmät, sovellukset, palvelut, liiketoimintaprosessit, toimittajat, henkilötietojen käsittelijät, alikäsittelijät, kansainväliset siirrot ja tietojen jakamista koskevat järjestelyt, jotka vaikuttavat PII:n käsittelyyn;

1.2.4 REG04:ssä ylläpidettävä tietosuojariskejä ja DPIA:ta koskeva todentava aineisto sekä REG02:ssa, REG03:ssa, REG08:ssa, REG09:ssä, REG10:ssä, REG11:ssä ja REG12:ssa ylläpidettävä tukeva todentava aineisto.

1.3 Tämä politiikka ei korvaa käsittelytoimien luetteloa koskevia kontrolleja, tietosuojaselostekontrolleja, suostumuskontrolleja, rekisteröidyn oikeuksien kontrolleja, sisäänrakennetun tietosuojan kontrolleja, toimittajakontrolleja, kansainvälisten siirtojen kontrolleja, PII:n tietoturvakontrolleja, poikkeamakontrolleja, dokumentoitua tietoa koskevia kontrolleja eikä seuranta-, auditointi- tai parantamiskontrolleja. Nämä vaatimukset määritetään kohdassa 12 luetelluissa liittyvissä politiikoissa.

1.4 Tässä politiikassa tietosuojariskien arviointi tarkoittaa PII:n käsittelystä mahdollisesti aiheutuvien haitallisten tietosuojavaikutusten dokumentoitua tunnistamista, analysointia, arviointia, käsittelyä, katselmointia ja seurantaa.

1.5 Tässä politiikassa DPIA tarkoittaa dokumentoitua arviointia, jota käytetään rekisterinpitäjän käsittelyssä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyille, ja jossa arvioidaan käsittelyn tarpeellisuus, oikeasuhteisuus, riskit, suojatoimet, jäännösriski, kuulemisen tarve ja hyväksynnän ehdot.

1.6 Tässä politiikassa korkea tietosuojaan kohdistuva jäännösriski tarkoittaa tietosuojariskiä, joka pysyy hyväksytyn hyväksymiskynnyksen yläpuolella ehdotetun tai toteutetun tietosuojariskien käsittelyn jälkeen.

1.7 Tässä politiikassa olennainen muutos tarkoittaa mitä tahansa muutosta, joka vaikuttaa PIMS:n soveltamisalaan, käsittelyn tarkoitukseen, oikeusperusteeseen, PII-ryhmiin, rekisteröityjen ryhmiin, käsittelyn laajuuteen, käsittelyteknologiaan, seurantaan tai profilointiin, automaattiseen päätöksentekoon, haavoittuvassa asemassa oleviin rekisteröityihin, vastaanottajiin, henkilötietojen käsittelijöihin, alikäsittelijöihin, kansainvälisiin siirtoihin, säilytykseen, tietoturvakontrolleihin, riskiprofiiliin, asiakkaan ohjeisiin tai sertifioinnin soveltamisalaan.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että tietosuojariskit ja DPIA-velvoitteet tunnistetaan, arvioidaan, käsitellään, hyväksytään, katselmoidaan ja osoitetaan todentavalla aineistolla ennen kuin PII:n käsittely aiheuttaa rekisteröidyille tai PIMS:lle riskin, jota ei voida hyväksyä.

2.2 Tämä politiikka auttaa organisaatiota osoittamaan riskiperusteista tietosuojan hallinnointia, rekisterinpitäjän DPIA:han liittyvää osoitusvelvollisuutta, henkilötietojen käsittelijän vaikutustenarvioinnissa avustamista, dokumentoitua riskien käsittelyä, jäännösriskin hyväksyntää, ennakkokuulemista koskevaa päätöksentekoa ja tietosuojakontrollien jatkuvaa parantamista.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 määrittää pakolliset tietosuojariskien esiarvioinnin käynnistysperusteet;

3.1.2 määrittää, milloin täysimittainen DPIA vaaditaan;

3.1.3 varmistaa, että rekisterinpitäjän DPIA-päätökset dokumentoidaan ja ovat katselmoitavissa;

3.1.4 varmistaa, että henkilötietojen käsittelijän ja alikäsittelijän vaikutustenarvioinnissa avustaminen dokumentoidaan, kun asiakkaan ohje tai sopimus sitä edellyttää;

3.1.5 varmistaa, että tietosuojariskit arvioidaan ennen uuden tai olennaisesti muuttuneen PII:n käsittelyn etenemistä;

3.1.6 varmistaa, että tietosuojariskien käsittelytoimet osoitetaan, toteutetaan ja varmennetaan;

3.1.7 varmistaa, että korkeat tietosuojaan kohdistuvat jäännösriskit eskaloidaan ja hyväksytään ennen käsittelyn aloittamista tai jatkamista;

3.1.8 varmistaa, että ennakkokuulemista koskevat päätökset dokumentoidaan, kun korkea jäännösriski säilyy;

3.1.9 varmistaa, että tietosuojariskejä ja DPIA:ta koskeva todentava aineisto ylläpidetään REG04:ssä ja linkitetään liittyviin todentavan aineiston kohteisiin;

3.1.10 välttää erillisten DPIA-, riski- tai kuulemisrekisterien luomista REG04:n ulkopuolelle.

4. Politiikkalausekkeet

4.1 Tietosuojariskien esiarviointi

4.1.1 [Both] Process Owner / Business Owner on käynnistettävä tietosuojariskien esiarviointi REG04:ssä ennen kuin REG02:een kirjattu uusi tai olennaisesti muuttunut PII:n käsittely alkaa.

4.1.2 [Both] Privacy Lead / PIMS Manager on ylläpidettävä tietosuojariskien esiarviointikriteerejä REG04:ssä ennen PIMS:n ensimmäistä käyttöönottoa ja sen jälkeen vuosittain.

4.1.3 [Controller] Process Owner / Business Owner on suoritettava DPIA-esiarviointi REG04:ssä ennen rekisterinpitäjän käsittelyä, joka täyttää tietosuojariskien esiarviointikriteerit.

4.1.4 [Processor] Vendor / Procurement Owner on kirjattava asiakkaan vaikutustenarvioinnissa avustamista koskevat vaatimukset REG08:aan ennen henkilötietojen käsittelijänä tehtävän käsittelyn aloittamista, kun asiakassopimus tai dokumentoitu ohje edellyttää DPIA-tukea.

4.1.5 [Both] System Owner / Application Owner on toimitettava järjestelmäsuunnittelua, käyttöoikeuksia, tietoturvaa, lokitusta ja tietovirtoja koskeva todentava aineisto REG04:ään ennen tietosuojariskien arvioinnin hyväksyntää uusille tai olennaisesti muuttuneille järjestelmille, joissa käsitellään PII:tä.

4.1.6 [Both] Privacy Lead / PIMS Manager on kirjattava esiarvioinnin tulos ja täysimittaista DPIA:ta koskevan päätöksen perustelut REG04:ään ennen käsittelytoimen etenemistä.

4.2 DPIA:n käynnistysperusteet ja vaatimuksen määrittäminen

4.2.1 [Controller] Privacy Lead / PIMS Manager on vaadittava täysimittaista DPIA:ta REG04:ssä ennen rekisterinpitäjän käsittelyä, joka todennäköisesti aiheuttaa korkean riskin.

4.2.2 [Controller] Process Owner / Business Owner on siirrettävä Privacy Lead / PIMS Managerin käsiteltäväksi REG04:ssä ennen käsittelyn aloittamista käsittely, johon liittyy laajamittaisuutta, järjestelmällistä seurantaa, profilointia, automaattisia päätöksiä, erityisiin henkilötietoryhmiin kuuluvaa PII:tä, rikostuomioihin tai rikkomuksiin liittyviä tietoja, haavoittuvassa asemassa olevia rekisteröityjä, innovatiivista teknologiaa tai olennaisesti muuttunutta käsittelyä.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor on kirjattava neuvonsa REG04:ään ennen korkean riskin rekisterinpitäjän käsittelyä koskevan täysimittaisen DPIA-vaatimuspäätöksen hyväksyntää.

4.2.4 [Both] Process Owner / Business Owner on esiarvioitava tietosuojariski uudelleen REG04:ssä ennen PII:n käyttämistä uuteen tarkoitukseen, uuden vastaanottajan lisäämistä, uuden henkilötietojen käsittelijän tai alikäsittelijän käyttöönottoa, järjestelmäarkkitehtuurin muuttamista tai uuden kansainvälisen siirron aloittamista.

4.2.5 [Processor] Privacy Lead / PIMS Manager on dokumentoitava REG08:ssa 10 työpäivän kuluessa asiakkaan vaikutustenarvioinnissa avustamista koskevan pyynnön vastaanottamisesta, edellytetäänkö henkilötietojen käsittelijältä DPIA-tukea.

4.2.6 [Subprocessor] Vendor / Procurement Owner on dokumentoitava REG08:ssa ylemmän tason vaikutustenarvioinnissa avustamista koskevat vaatimukset ennen alikäsittelyn aloittamista, kun ylemmän tason asiakkaan tai henkilötietojen käsittelijän sopimus edellyttää tällaista avustamista.

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

9. Poikkeukset

9.1 Tietosuojariskejä ja DPIA:ta koskevat poikkeukset

9.1.1 [All] Process Owner / Business Owner on pyydettävä kaikki tätä politiikkaa koskevat poikkeukset REG12:ssa ennen poikkeaman tapahtumista.

9.1.2 [All] Privacy Lead / PIMS Manager on arvioitava kunkin pyydetyn poikkeuksen tietosuoja-, oikeudelliset, sertifiointi-, operatiiviset ja rekisteröityihin kohdistuvat vaikutukset REG04:ssä tai REG12:ssa 10 työpäivän kuluessa pyynnöstä.

9.1.3 [All] Data Protection Officer / Privacy Advisor on kirjattava neuvonsa REG12:een ennen sellaisen poikkeuksen hyväksyntää, joka vaikuttaa korkean riskin käsittelyyn, täysimittaisen DPIA:n valmistumiseen, ennakkokuulemiseen, korkeaan tietosuojaan kohdistuvaan jäännösriskiin tai asiakkaan vaikutustenarvioinnissa avustamiseen.

9.1.4 [All] Top Management on hyväksyttävä tietosuojariski- tai DPIA-poikkeukset, jotka vaikuttavat korkean riskin käsittelyyn, sertifioinnin soveltamisalaan, ennakkokuulemiseen tai ratkaisemattomaan korkeaan tietosuojaan kohdistuvaan jäännösriskiin, REG12:ssa ennen poikkeuksen voimaantuloa.

9.1.5 [All] Privacy Lead / PIMS Manager on asetettava REG12:ssa kullekin hyväksytylle tietosuojariski- tai DPIA-poikkeukselle enintään 90 päivän päättymispäivä ennen hyväksyntää.

9.1.6 [All] Process Owner / Business Owner on suljettava tai arvioitava uudelleen kukin tietosuojariski- tai DPIA-poikkeus REG12:ssa viiden työpäivän kuluessa päättymisestä.

10. Soveltaminen

10.1 Tietosuojariskien ja DPIA:n soveltaminen

10.1.1 [All] Privacy Lead / PIMS Manager on kirjattava puuttuva, virheellinen, epätäydellinen, myöhässä oleva tai hyväksymätön REG04:n tietosuojariski- tai DPIA-todentava aineisto poikkeamana REG12:ssa viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [Controller] Process Owner / Business Owner on keskeytettävä uusi korkean riskin rekisterinpitäjän käsittely, kun vaadittu REG04:n DPIA-hyväksyntää koskeva todentava aineisto puuttuu ennen käyttöönottoa.

10.1.3 [Both] System Owner / Application Owner on estettävä PII:tä käsittelevien järjestelmien tuotantokäyttöönotto, kun vaadittu REG04:n riskien käsittelyä koskeva todentava aineisto puuttuu ennen tuotantokäyttöönoton hyväksyntää.

10.1.4 [Both] Vendor / Procurement Owner on estettävä toimittajan, henkilötietojen käsittelijän, alikäsittelijän tai tietojen jakamista koskevan järjestelyn käyttöönotto, kun vaadittu REG04:n tietosuojariski- tai vaikutustenarvioinnissa avustamista koskeva todentava aineisto puuttuu ennen sopimuksen hyväksyntää.

10.1.5 [All] Top Management on katselmoitava ratkaisemattomat merkittävät tietosuojariski- tai DPIA-poikkeamat REG12:ssa johdon katselmoinnin aikana.

10.1.6 [All] Privacy Lead / PIMS Manager on eskaloitava toistuvat REG04-esiarvioinnin, DPIA-katselmoinnin tai riskien käsittelyn määräaikojen laiminlyönnit Top Managementille REG12:ssa viiden työpäivän kuluessa toisesta esiintymästä 12 kuukauden jaksolla.

10.1.7 [All] Internal Audit / Compliance Reviewer on varmennettava tietosuojariski- ja DPIA-poikkeamia koskevien korjaavien toimenpiteiden tehokkuus REG12:ssa seuraavassa ajoitetussa 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 on katselmoitava tämä politiikka REG12:ssa vuosittain ja 30 päivän kuluessa olennaisesta muutoksesta tietosuojariskiä, DPIA:ta, ennakkokuulemista, henkilötietojen käsittelijän avustamista tai sertifiointivaatimuksia koskien.

11.1.2 [All] Privacy Lead / PIMS Manager on katselmoitava REG04:n esiarviointikriteerit, DPIA:n käynnistyskriteerit, riskiluokituskriteerit ja jäännösriskin hyväksymiskriteerit REG12:ssa vuosittain.

11.1.3 [All] Data Protection Officer / Privacy Advisor on katselmoitava tähän politiikkaan tehtävät tietosuojan kannalta merkittävät muutokset REG12:ssa ennen hyväksyntää.

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

11.1.5 [All] Privacy Lead / PIMS Manager on päivitettävä REG03 ja REG04 15 työpäivän kuluessa hyväksytyistä politiikkamuutoksista, jotka muuttavat kontrollien soveltuvuutta, riskikriteerejä tai DPIA-esiarviointivaatimuksia.

11.1.6 [All] Privacy Lead / PIMS Manager on kirjattava tämän politiikan hyväksyttyjen muutosten viestintä 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 PII03 - PII:n käsittelytoimien luettelon ja oikeusperusteen politiikka

12.5 PII04 - Tietosuojaseloste- ja läpinäkyvyyspolitiikka

12.6 PII05 - Suostumuksen ja valinta-asetusten hallintapolitiikka

12.7 PII06 - Rekisteröidyn oikeuksien hallintapolitiikka

12.8 PII08 - Sisäänrakennetun ja oletusarvoisen tietosuojan politiikka

12.9 PII09 - PII:n keräämisen, käytön, luovuttamisen ja jakamisen politiikka

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

12.11 PII11 - PII:n oikeellisuus- ja laatupolitiikka

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

12.13 PII13 - Kansainvälisten PII-siirtojen politiikka

12.14 PII14 - PII:n tietoturva- ja pääsynhallintapolitiikka

12.15 PII15 - PII-poikkeamien ja tietoturvaloukkausten hallintapolitiikka

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

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

13. Viitestandardit ja viitekehykset

13.1 Tämä politiikka on kartoitettu seuraaviin standardeihin ja säädöksiin. Kartoitus selittää, miten politiikka tukee viitattuja vaatimuksia ja yksilöi sisäiset lausekkeet, jotka toteuttavat tai tukevat niitä.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Kartoitettu tietosuojariskejä ja mahdollisuuksia koskevien toimien tunnistamiseen ja suunnitteluun käyttäen esiarviointikriteerejä, riskikynnyksiä, eskalointia ja johdon katselmoinnin syötteitä. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Kartoitettu tietosuojariskien esiarvioinnin, tietosuojariskien arvioinnin, riskiluokituksen, uudelleenarvioinnin ja DPIA:n käynnistysperusteiden arvioinnin suorittamiseen ennen uuden tai olennaisesti muuttuneen käsittelyn etenemistä. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Kartoitettu tietosuojariskien käsittelyn suunnitteluun, kontrollien soveltuvuuspäivityksiin, käsittelyn toteuttamiseen, jäännösriskin hyväksyntään ja SoA-yhteyteen. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Kartoitettu suunniteltuihin PIMS- ja käsittelymuutoksiin, jotka käynnistävät tietosuojariskien uudelleenarvioinnin ja DPIA-katselmoinnin. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Kartoitettu hallittuun dokumentoituun tietoon tietosuojariskien esiarvioinnista, DPIA:n todentavasta aineistosta, riskien käsittelystä, jäännösriskin hyväksynnästä, ennakkokuulemista koskevista päätöksistä, poikkeuksista, poikkeamista ja politiikan katselmointiaineistosta. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Kartoitettu tietosuojariskien ja DPIA:n kontrollien käyttöön ennen tuotantokäyttöönottoa, käyttöönottoa, käsittelyn hyväksyntää, käsittelytoimen sulkemista ja korjaavaan toimenpiteeseen linkittämistä. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Kartoitettu operatiiviseen tietosuojariskien arviointiin uusien, muuttuneiden, järjestelmiin, toimittajiin, siirtoihin ja poikkeamiin liittyvien käsittelymuutosten osalta. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Kartoitettu operatiiviseen tietosuojariskien käsittelyyn, käsittelytoimien osoittamiseen, käsittelytoimien toteuttamiseen, myöhässä olevien käsittelytoimien eskalointiin ja tehokkuuden varmentamiseen. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Kartoitettu esiarvioinnin kattavuuden, DPIA:n tilan, avoimien riskien, myöhässä olevien käsittelytoimien, toimittajatoimien, tietoturvan käsittelytoimien, poikkeamien uudelleenarviointitoimien ja auditointihavaintojen seurantaan ja mittaamiseen. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Kartoitettu korkeiden tietosuojaan kohdistuvien jäännösriskien, myöhässä olevien käsittelytoimien, täysimittaisen DPIA:n tilan, ennakkokuulemista koskevien päätösten ja merkittävien tietosuojariskipoikkeusten johdon katselmointiin. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Kartoitettu tietosuojariski- ja DPIA-poikkeamiin, poikkeuksiin, korjaavan toimenpiteen avaamiseen, eskalointiin ja tehokkuuden varmentamiseen. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Kartoitettu tietosuojaa koskevan vaikutustenarvioinnin tarpeen arviointiin ja tarvittaessa toteuttamiseen uudessa tai muuttuneessa rekisterinpitäjän käsittelyssä. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Kartoitettu käsittelytoimien tallenteisiin, jotka tukevat tietosuojariskien ja DPIA:n arvioinnin syötteitä, mukaan lukien tarkoitus, ryhmät, järjestelmät, vastaanottajat, siirrot ja toimittajat. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Kartoitettu henkilötietojen käsittelijän asiakassopimuksiin ja asiakkaan vaikutustenarvioinnissa avustamista koskeviin velvoitteisiin. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Kartoitettu siihen, että henkilötietojen käsittelijä antaa asiakkaan vaatimustenmukaisuuteen tarvittavat tiedot, mukaan lukien vaikutustenarvioinnissa avustaminen ja asiakastuen todentava aineisto. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Kartoitettu osoitusvelvollisuuden todentavaan aineistoon DPIA-esiarvioinnista, täysimittaista DPIA:ta koskevista päätöksistä, riskien käsittelystä, jäännösriskin hyväksynnästä, ennakkokuulemista koskevista päätöksistä, poikkeuksista, auditointihavainnoista ja korjaavista toimenpiteistä. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän vastuuseen asianmukaisista tietosuojariskien toimenpiteistä, korkean jäännösriskin katselmoinnista, johdon hyväksynnästä ja politiikan ylläpidosta. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Kartoitettu sisäänrakennetun ja oletusarvoisen tietosuojan todentavaan aineistoon, jota käytetään riskien arvioinnissa ja ennen tuotantokäyttöönoton hyväksyntää. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Kartoitettu henkilötietojen käsittelijän ja alikäsittelijän vaikutustenarvioinnissa avustamiseen, asiakkaan ohjeiden käsittelyyn ja toimittajariskien käsittelyä koskevaan todentavaan aineistoon. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Kartoitettu käsittelytoimien tallenteisiin, jotka tukevat tietosuojariskien arvioinnin ja DPIA:n syötteitä. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Kartoitettu PII:n tietoturvariskien syötteisiin, suojatoimien valintaan, tietoturvariskien käsittelyyn ja tietoturvakontrollien tilapäivityksiin. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Kartoitettu DPIA-esiarviointiin, täysimittaisen DPIA-vaatimuksen määrittämiseen, DPIA:n sisältöön, DPO-neuvontaan, katselmointiin ja korkean riskin käsittelyn estämiseen ilman vaadittua DPIA-hyväksyntää. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Kartoitettu ennakkokuulemista koskevaan päätöksentekoon, DPO-neuvontaan, Top Managementin hyväksyntään sekä jatkamista, keskeyttämistä, uudelleensuunnittelua tai kuulemista koskeviin toimiin, kun korkea jäännösriski säilyy. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Kartoitettu Data Protection Officer / Privacy Advisor -neuvontaan ja seurantaan soveltuvin osin DPIA-päätöksissä, korkean riskin käsittelyssä, ennakkokuulemisessa ja politiikkamuutoksissa. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Kartoitettu tietosuojakontrollien tunnistamiseen, tietoturvasuojatoimiin, tietosuojavaatimusten noudattamiseen, tietosuojariskien todentavaan aineistoon, seurantaan ja katselmointiin. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Kartoitettu PIA-prosessin soveltamisalaan, hyötyihin, käynnistysperusteen määrittämiseen, valmisteluun, arvioinnin syötteisiin, sidosryhmiä koskevaan todentavaan aineistoon ja REG04:ssä ylläpidettävään DPIA-raportin rakenteeseen. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Kartoitettu PII:n suojausohjelman vaatimuksiin, PII:n suojausvaatimusten tunnistamiseen, riskiperusteiseen hallintakeinojen valintaan ja tietosuojariskien käsittelyn yhteyteen. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Kartoitettu organisaation tietosuojariskien periaatteisiin, johtajuuteen, integrointiin, riskien arviointiin, riskien käsittelyyn, seurantaan ja katselmointiin sekä kirjaamiseen ja raportointiin. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].