					Lisää tähän rekisteröidyn oikeushenkilön nimi							
Asiakirjan numero: PII08					Asiakirjan nimi: **Sisäänrakennetun ja oletusarvoisen tietosuojan 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 6.1.2; Clause 6.1.3	Both	Supporting	Tietosuojariskien arvioinnin ja käsittelyn yhteys
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Suunnitellut muutokset ja operatiivinen kontrolli
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentoitu sisäänrakennetun tietosuojan todentava aineisto
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Tarkoitukset, PIA-heräte ja tallenteet
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Keräämisen ja käsittelyn rajoittaminen
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Oikeellisuutta ja minimointia koskevat tavoitteet
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Tunnistamattomaksi tekeminen, poistamisen suunnittelu ja väliaikaiset tiedostot
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Asiakassopimus, tuki ja henkilötietojen käsittelijän tallenteet
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Henkilötietojen käsittelijän suunnitteluvalmiudet
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Kehityksen elinkaari ja suunnitteluperiaatteet
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Käyttötarkoitussidonnaisuus, minimointi ja osoitusvelvollisuus
GDPR	Article 24	Controller	Supporting	Rekisterinpitäjän toimenpiteet
GDPR	Article 25	Controller	Primary	Sisäänrakennettu ja oletusarvoinen tietosuoja
GDPR	Article 28	Both	Supporting	Henkilötietojen käsittelijän ohjeet ja avustaminen
GDPR	Article 30	Both	Supporting	Käsittelytoimien tallenteet

GDPR	Article 35	Controller	Supporting	DPIA-herätteen yhteys
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Tietosuojakontrollit suunnittelun kautta
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Tarkoitus, kerääminen, minimointi ja käytön rajoittaminen
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Oikeellisuus, osoitusvelvollisuus ja vaatimustenmukaisuus
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	PII:n suojaamisen periaatteet ja kontrollit

1. Soveltamisala

1.1 Tämä politiikka määrittää vaatimukset sisäänrakennetun tietosuojan ja oletusarvoisen tietosuojan sisällyttämiseksi uusiin ja muutettuihin PII:n käsittelytoimiin, projekteihin, tuotteisiin, palveluihin, järjestelmiin, sovelluksiin, integraatioihin, hankintatoimiin ja liiketoimintaprosessien muutoksiin PIMS:n soveltamisalassa.

1.2 Tätä politiikkaa sovelletaan rekisterinpitäjän, yhteisrekisterinpitäjän, henkilötietojen käsittelijän ja alikäsittelijän toimintaympäristöihin.

1.3 Henkilötietojen käsittelijää ja alikäsittelijää koskevia velvoitteita sovelletaan, kun organisaatio suunnittelee, konfiguroi, muuttaa tai käyttää käsittelyä asiakkaan, rekisterinpitäjän tai ylemmän tason henkilötietojen käsittelijän puolesta dokumentoitujen ohjeiden mukaisesti.

1.4 Tämä politiikka kattaa:

1.4.1 tietosuojavaatimukset projektin käynnistämisessä;

1.4.2 tarkoitusta, tietojen minimointia ja oletusasetuksia koskevat suunnittelukontrollit;

1.4.3 sisäänrakennetun tietosuojan katselmoinnin ennen tuotantokäyttöönottoa;

1.4.4 muutoksesta käynnistyvän sisäänrakennetun tietosuojan katselmoinnin;

1.4.5 hankinnan sisäänrakennetun tietosuojan tarkastukset;

1.4.6 yhteyden tietosuojariskiin, DPIA-esiarviointiin ja korjaavia toimenpiteitä koskevaan todentavaan aineistoon.

1.5 Tämä politiikka ei korvaa:

1.5.1 PII03-politiikkaa käsittelytoimien luettelon, tarkoitusten, oikeusperusteen ja ROPA-tallenteiden osalta;

1.5.2 PII04-politiikkaa tietosuojaselosteen sisällön ja julkaisemisen osalta;

1.5.3 PII05-politiikkaa suostumus- ja valinta-asetuskontrollien osalta;

1.5.4 PII06-politiikkaa rekisteröityjen oikeuksien käsittelyn osalta;

1.5.5 PII07-politiikkaa tietosuojariskien arvioinnin ja DPIA:n menetelmän osalta;

1.5.6 PII09-politiikkaa keräämistä, käyttöä, luovuttamista ja jakamista koskevien kontrollien osalta;

1.5.7 PII10-politiikkaa säilytyksen, poistamisen ja hävittämisen toteutuksen osalta;

1.5.8 PII11-politiikkaa oikeellisuuden ja laadun operatiivisen toiminnan osalta;

1.5.9 PII12-politiikkaa henkilötietojen käsittelijöiden, alikäsittelijöiden ja kolmansien osapuolten elinkaaren hallinnoinnin osalta;

1.5.10 PII13-politiikkaa kansainvälisten PII-siirtojen mekanismien osalta;

1.5.11 PII14-politiikkaa PII:n turvallisuuden ja pääsynhallinnan operatiivisen toiminnan osalta;

1.5.12 PII18-politiikkaa koko PIMS:n seurannan, auditoinnin, korjaavien toimenpiteiden ja parantamisen hallinnoinnin osalta.

2. Tarkoitus

2.1 Tämän politiikan tarkoituksena on varmistaa, että tietosuojavaatimukset tunnistetaan, toteutetaan ja osoitetaan todentavalla aineistolla ennen PII:n käsittelyn aloittamista tai olennaista muuttamista ja että järjestelmät ja prosessit konfiguroidaan oletusarvoisesti rajoittamaan PII:n kerääminen, käyttö, altistuminen, säilytysriippuvuus, luovutusriippuvuus ja tunnistettavuus siihen, mikä on dokumentoidun tarkoituksen kannalta tarpeellista.

3. Tavoitteet

3.1 Tämän politiikan tavoitteena on:

3.1.1 sisällyttää tietosuojavaatimukset projektin käynnistämistä, suunnittelua, hankintaa, muutosta ja tuotantokäyttöönottoa koskeviin päätöksiin;

3.1.2 varmistaa, että PII:n käsittelyn suunnitteluratkaisut liittyvät dokumentoituihin tarkoituksiin ja REG02-käsittelytallenteisiin;

3.1.3 toteuttaa tietojen minimointi ja tietosuojaa edistävät oletusasetukset ennen käsittelyn aloittamista;

3.1.4 varmistaa tietosuojariskin ja DPIA-esiarvioinnin käynnistyminen ilman PII07-menetelmän päällekkäistä toistamista;

3.1.5 varmistaa, että hankintaa ja henkilötietojen käsittelijän suunnittelua koskevat vaatimukset kirjataan ilman PII12-elinkaaren hallinnoinnin päällekkäistä toistamista;

3.1.6 varmistaa, että ratkaisemattomat suunnittelukysymykset eskaloidaan REG12:n kautta;

3.1.7 ylläpitää auditointia varten valmista suunnittelun todentavaa aineistoa REG02:ssa, REG04:ssa, REG08:ssa ja REG12:ssa.

4. Politiikkalausumat

4.1 Projektin käynnistäminen ja tietosuojavaatimukset

4.1.1 [Both] Process Owner / Business Owner tulee kirjata sisäänrakennetun tietosuojan kirjaus REG04:ään ennen minkä tahansa PII:tä sisältävän projektin, tuotteen, palvelun, järjestelmän, sovelluksen, integraation tai liiketoimintaprosessin muutoksen käynnistämistä.

4.1.2 [Both] Process Owner / Business Owner tulee linkittää jokainen REG04:n sisäänrakennetun tietosuojan kirjaus olemassa olevaan tai luonnosvaiheessa olevaan REG02-käsittelytoimeen ennen toiminnallisten vaatimusten hyväksymistä.

4.1.3 [Controller] Privacy Lead / PIMS Manager tulee kirjata rekisterinpitäjän sisäänrakennettua tietosuojaa koskevat vaatimukset REG04:ään ennen rekisterinpitäjän toiminnallisen suunnittelun hyväksymistä.

4.1.4 [Processor] Vendor / Procurement Owner tulee kirjata asiakkaan tietosuojasuunnittelua koskevat ohjeet ja sopimusperusteiset suunnittelurajoitteet REG08:aan ennen henkilötietojen käsittelijän palvelusuunnittelun tai olennaisen palvelumuutoksen hyväksymistä.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor tulee kirjata neuvonta REG04:ään ennen korkean riskin, uudenlaisen, arkaluonteisen, automatisoidun, laajamittaisen tai olennaisesti muutetun PII-suunnittelun hyväksymistä.

4.1.6 [Both] Information Security Lead tulee kirjata tietosuojasuunnittelua tukevat PII:n tietoturvakontrollien riippuvuudet REG04:ään ennen arkkitehtuurin hyväksymistä.

4.2 Tietojen minimointi ja oletusarvoisen tietosuojan suunnittelu

4.2.1 [Controller] Process Owner / Business Owner tulee dokumentoida PII-luokkien, rekisteröityjen ryhmien, lähteiden ja tarkoitusten vähimmäislaajuus REG02:ssa ja REG04:ssa ennen keräämisen tai tuonnin suunnittelun hyväksymistä.

4.2.2 [Both] System Owner / Application Owner tulee konfiguroida käsittelyn oletusasetukset siten, että PII:n kerääminen ja käsittely rajoittuvat dokumentoidun tarkoituksen edellyttämään vähimmäistasoon, ja kirjata todentava aineisto REG04:ään ennen tuotantokäyttöönottoa.

4.2.3 [Controller] Process Owner / Business Owner tulee dokumentoida valinnaiset PII-kentät, valinnaiset käsittelyvalinnat ja oletusarvoisesti pois päältä olevat asetukset REG02:ssa ja REG04:ssa ennen käyttöliittymän, lomakkeen tai työnkulun hyväksymistä.

4.2.4 [Both] System Owner / Application Owner tulee dokumentoida näkymien, raporttien, vientien, rajapintojen ja automatisoitujen työnkulkujen oletusarvoiset tietosuojan altistusasetukset REG04:ään ennen tuotantokäyttöönottoa.

4.2.5 [Both] Process Owner / Business Owner tulee dokumentoida tunnistamattomaksi tekemisen, pseudonymisoinnin, aggregoinnin tai ei-tunnistettavan käsittelyn toteuttamiskelpoisuus REG04:ään ennen tunnistettavissa olevan PII:n hyväksymistä testaukseen, analytiikkaan, raportointiin tai toissijaiseen operatiiviseen käyttöön.

4.2.6 [Both] System Owner / Application Owner tulee dokumentoida väliaikaisten henkilötietoartefaktien käsittely, mukaan lukien väliaikaiset tiedostot, välimuistit, lokit tai staging-tallenteet, REG04:ään ennen tuotantokäyttöönottoa.

4.2.7 [Both] Process Owner / Business Owner tulee ohjata PII10-, PII11-, PII13- tai PII14-politiikan omistamat suunnitteluvaatimukset asiaankuuluvaan politiikan todentavan aineiston polkuun REG04:ssä viiden työpäivän kuluessa riippuvuuden tunnistamisesta.

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

9. Poikkeukset

9.1 Tietosuojasuunnittelun poikkeukset

9.1.1 [Both] Process Owner / Business Owner tulee pyytää tietosuojasuunnittelun poikkeus REG12:ssa ennen sellaisen suunnittelun tai muutoksen hyväksymistä, joka ei voi täyttää sovellettavaa tietosuojasuunnittelun vaatimusta.

9.1.2 [Both] Privacy Lead / PIMS Manager tulee arvioida kunkin tietosuojasuunnittelun poikkeuksen vaikutus, korvaavat kontrollit ja voimassaolon päättyminen REG12:ssa viiden työpäivän kuluessa pyynnöstä.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor tulee kirjata neuvonta REG12:een ennen sellaisen tietosuojasuunnittelun poikkeuksen hyväksymistä, joka koskee korkean riskin, arkaluonteista, automatisoitua, laajamittaista, riidanalaista tai oikeudellisesti olennaista käsittelyä.

9.1.4 [All] Top Management tulee hyväksyä suuren vaikutuksen käsittelyyn, sertifioinnin soveltamisalaan, ratkaisemattomaan merkittävään riskiin tai lakisääteiseen velvoitteeseen vaikuttava tietosuojasuunnittelun poikkeus REG12:ssa ennen poikkeuksen voimaantuloa.

9.1.5 [Both] Privacy Lead / PIMS Manager tulee asettaa kullekin hyväksytylle tietosuojasuunnittelun poikkeukselle REG12:ssa viimeinen voimassaolopäivä, joka on enintään 90 päivää hyväksymisestä.

9.1.6 [Both] Privacy Lead / PIMS Manager tulee sulkea tai arvioida uudelleen kukin tietosuojasuunnittelun poikkeus REG12:ssa viiden työpäivän kuluessa sen voimassaolon päättymisestä.

10. Soveltaminen

10.1 Soveltaminen ja poikkeamien käsittely

10.1.1 [Both] Privacy Lead / PIMS Manager tulee kirjata puuttuva sisäänrakennetun tietosuojan katselmointi, puuttuva minimoinnin todentava aineisto, ratkaisematon oletusasetuksen puute tai luvaton tuotantokäyttöönotto poikkeamana REG12:een viiden työpäivän kuluessa tunnistamisesta.

10.1.2 [Both] System Owner / Application Owner tulee estää PII:tä käsittelevän järjestelmän tuotantokäyttöönotto, jos REG04:n sisäänrakennetun tietosuojan katselmointi on keskeneräinen, ja kirjata päätös REG12:een ennen tuotantokäyttöönottoa.

10.1.3 [Both] Vendor / Procurement Owner tulee estää toimittajan käyttöönotto tai sopimuksen allekirjoittaminen, jos vaadittu REG08:n tietosuojasuunnittelun todentava aineisto puuttuu, ja kirjata päätös REG12:een ennen käyttöönottoa tai allekirjoittamista.

10.1.4 [Both] Process Owner / Business Owner tulee keskeyttää uuden tai muutetun PII:n käsittelysuunnittelun käyttö, kunnes REG04-katselmointi, REG02-päivitykset ja vaaditut REG12-poikkeukset on saatettu valmiiksi.

10.1.5 [All] Top Management tulee edellyttää korjaavaa toimenpidettä REG12:ssa 10 työpäivän kuluessa toistuvan, pitkittyneen tai suuren vaikutuksen tietosuojasuunnittelun epäonnistumisen osalta.

10.1.6 [All] Internal Audit / Compliance Reviewer tulee varmistaa tietosuojasuunnittelun poikkeamia koskevien korjaavien toimenpiteiden tehokkuus REG12:ssa seuraavassa aikataulutetussa PIMS-auditoinnissa tai 60 päivän kuluessa sulkemisesta sen mukaan, kumpi tapahtuu ensin.

11. Katselmointi ja ylläpito

11.1 Politiikan ja suunnittelukontrollien katselmointi

11.1.1 [All] Privacy Lead / PIMS Manager tulee katselmoida tämä politiikka REG12:ssa vuosittain ja 30 päivän kuluessa olennaisesta lainsäädännön, käsittelyn, teknologian, sertifioinnin soveltamisalan tai PIMS-kontrollin muutoksesta.

11.1.2 [Both] Process Owner / Business Owner tulee katselmoida aktiiviset REG02-käsittelytoimet tietosuojasuunnittelun riippuvuuksien muutosten osalta vuosittain ja 30 päivän kuluessa olennaisesta käsittelymuutoksesta.

11.1.3 [Both] System Owner / Application Owner tulee katselmoida oletusarvoisen tietosuojan konfiguraation todentava aineisto REG04:ssä vuosittain ja 30 päivän kuluessa olennaisesta järjestelmämuutoksesta.

11.1.4 [Both] Vendor / Procurement Owner tulee katselmoida toimittajia, henkilötietojen käsittelijöitä, alikäsittelijöitä ja kolmansia osapuolia koskevat tietosuojasuunnittelun velvoitteet REG08:ssa ennen uusimista ja 30 päivän kuluessa olennaisesta suhteen muutoksesta.

11.1.5 [Conditional] Data Protection Officer / Privacy Advisor tulee arvioida olennaisten politiikkamuutosten tietosuojavaikutus REG12:ssa ennen hyväksymistä.

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

12. Liittyvät politiikat

12.1 PII01 - Henkilötietojen hallintajärjestelmäpolitiikka

12.2 PII02 - Tietosuojaa koskevien roolien, vastuiden ja osoitusvelvollisuuden politiikka

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

12.4 PII04 - Tietosuojaselostetta ja läpinäkyvyyttä koskeva politiikka

12.5 PII05 - Suostumuksen ja valinta-asetusten hallintapolitiikka

12.6 PII06 - Rekisteröityjen oikeuksien hallintapolitiikka

12.7 PII07 - Tietosuojariskien arvioinnin ja DPIA:n 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 tietosuojanhallintapolitiikka

12.12 PII13 - Kansainvälisten PII-siirtojen politiikka

12.13 PII14 - PII:n tietoturva- 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 kartoitettu seuraaviin standardeihin ja säädöksiin. Kartoitus selittää, miten politiikka tukee viitattuja vaatimuksia, ja yksilöi sisäiset lausekkeet, joilla ne toteutetaan tai joita ne tukevat.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.2; Clause 6.1.3** - Kartoitettu tietosuojariskin esiarviointiin, käsittelytoimien yhteyteen, suunnitteluriippuvuuksien analyysiin, eskalointiin ja korjaaviin toimenpiteisiin ilman koko tietosuojariskien arvioinnin ja DPIA-menetelmän päällekkäistä toistamista. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Kartoitettu suunniteltuihin tietosuojamuutoksiin, projektin käynnistämiseen, operatiiviseen sisäänrakennetun tietosuojan katselmointiin, tuotantokäyttöönoton valvontaan ja olennaisen muutoksen katselmointiin. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Kartoitettu dokumentoituun sisäänrakennetun tietosuojan todentavaan aineistoon, joka säilytetään REG02:ssa, REG04:ssä, REG08:ssa ja REG12:ssa. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Kartoitettu tietosuojasuunnittelun mittareihin, todentavan aineiston otantaan, poikkeamien kirjaamiseen, korjaaviin toimenpiteisiin ja tehokkuuden varmistamiseen. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Kartoitettu käsittelyn tarkoitusten dokumentointiin, käsittelytallenteisiin, sisäänrakennetun tietosuojan yhteyteen sekä tietosuojariskin tai DPIA-esiarvioinnin herätteisiin rekisterinpitäjän käsittelyssä. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Kartoitettu PII:n keräämisen ja käsittelyn rajoittamiseen tarkoitusperusteisten vähimmäistietovaatimusten, oletusarvoisesti pois päältä olevien valinnaisten käsittelyjen ja oletuskäsittelyn vähimmäisasetusten avulla. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Kartoitettu oikeellisuusriippuvuuden ohjaukseen, minimointitavoitteisiin, tunnistamattomaksi tekemisen toteuttamiskelpoisuuteen ja tunnistettavissa olevan PII:n minimointia koskevaan suunnittelun todentavaan aineistoon. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Kartoitettu tunnistamattomaksi tekemisen, poistamisriippuvuuden ja väliaikaisten henkilötietoartefaktien tunnistamiseen suunnitteluvaiheessa sekä ohjaukseen elinkaarikontrolleihin ilman säilytyksen tai hävittämisen toteutuksen päällekkäistä toistamista. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Kartoitettu henkilötietojen käsittelijän asiakkaan ohjeisiin, asiakastuen tietoihin, henkilötietojen käsittelijän suunnittelutallenteisiin ja asiakkaan valtuuttamiin palvelusuunnittelun muutoksiin. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Kartoitettu henkilötietojen käsittelijän suunnitteluvalmiuksiin väliaikaisten tiedostojen, palautus- tai hävittämisriippuvuuden ja siirron valvonnan riippuvuuden osalta, jotka kirjataan suunnittelun todentavana aineistona ilman operatiivisten poisto- tai tietoturvakontrollimenettelyjen päällekkäistä toistamista. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Kartoitettu tietosuojavaatimuksiin kehityksen elinkaaressa, suunnitteluperiaatteisiin, PII:n suojaamisen tarkastuspisteisiin ja oletusarvoisen tietosuojan konfiguraation todentavaan aineistoon. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Kartoitettu käyttötarkoitussidonnaisuuteen, PII:n vähimmäislaajuuden suunnitteluun, käsittelytallenteiden yhteyteen, oletusarvoiseen minimointiin, todentavaan aineistoon ja osoitusvelvollisuuteen. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Kartoitettu rekisterinpitäjän toimenpiteisiin, hallinnoinnin katselmointiin, poikkeuksen hyväksymiseen, korjaaviin toimenpiteisiin ja politiikan ylläpitoon sisäänrakennetun tietosuojan toteutuksessa. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Kartoitettu projektin käynnistämiseen, suunnitteluvaiheen tietosuojavaatimuksiin, oletusarvoisen tietosuojan asetuksiin, minimointiin, hankinnan suunnittelutarkastuksiin, tuotantokäyttöönoton katselmointiin ja muutoksesta käynnistyvään katselmointiin. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Kartoitettu henkilötietojen käsittelijän ohjeisiin, henkilötietojen käsittelijän suunnittelutukeen, toimittajan tietosuojasuunnittelun todentavaan aineistoon ja asiakkaan valtuuttamiin suunnittelumuutoksiin. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Kartoitettu käsittelytallenteiden yhteyteen, REG02-päivityksiin, käsittelytoimen suunnitteluriippuvuuksiin ja käsittelytallenteiden todentavaan aineistoon. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Kartoitettu suunnitteluvaiheen tietosuojariskin ja DPIA-esiarvioinnin herätteisiin, korkean riskin neuvontaan ja toteutuksen jälkeisiin tarkastuksiin ilman DPIA-menetelmän päällekkäistä toistamista. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Kartoitettu tietosuojakontrollien tunnistamiseen suunnitteluvaiheessa, tietosuojariskin yhteyteen ja kontrollien toteutusta koskevaan suunnittelun todentavaan aineistoon. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kartoitettu tarkoituksen määrittelyyn, keräämisen rajoittamiseen, tietojen minimointiin, käytön rajoittamiseen ja käsittelyn oletusasetuksiin. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Kartoitettu oikeellisuusriippuvuuden ohjaukseen, osoitusvelvollisuuden todentavaan aineistoon, tietosuojasuunnittelun seurantaan, auditointiin ja korjaaviin toimenpiteisiin. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Kartoitettu tarkoituksen lainmukaisuuteen, keräämisen rajoittamiseen, tietojen minimointiin, käytön ja luovuttamisen rajoittamiseen, säilytysriippuvuuteen, väliaikaisten tiedostojen käsittelyyn ja oikeellisuusriippuvuuden suunnittelukontrolleihin. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].