					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII03					Dokumenttitel: **Policy för PII-behandlingsförteckning och rättslig grund**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / regelverk	Klausul / kontroll / artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	Fastställande av PIMS-roll för behandlingsaktiviteter
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Koppling till utlösare för riskbedömning av integritetsrisker
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Koppling till kontrolltillämplighet och SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterad information för behandlingsförteckning
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operativ planering och styrning av behandlingsposter
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Koppling till operativ riskbedömning av integritetsrisker
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Övervakning och mätning av förteckningen
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Avvikelse och korrigerande åtgärder för förteckningen
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Identifiering av ändamål för personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Identifiering av rättslig grund för personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Koppling till screening för DPIA
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Register över behandlingsansvar för gemensamt personuppgiftsansvar
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Register för personuppgiftsansvarig avseende behandling av PII

ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Kundavtal och instruktionsunderlag för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Anpassning av personuppgiftsbiträdets ändamål till kundinstruktioner
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Register för personuppgiftsbiträde avseende behandling av PII
GDPR	Article 5(1)(a)	Controller	Supporting	Koppling till laglighet, korrekthet och transparens
GDPR	Article 5(1)(b)	Controller	Supporting	Ändamålsbegränsning
GDPR	Article 5(1)(c)	Controller	Supporting	Uppgiftsminimering
GDPR	Article 5(1)(e)	Controller	Supporting	Koppling till lagringsbegränsning
GDPR	Article 5(2)	Controller	Supporting	Underlag för ansvarsskyldighet
GDPR	Article 6	Controller	Primary	Laglighet vid behandling
GDPR	Article 9	Conditional	Supporting	Villkor för behandling av särskilda kategorier
GDPR	Article 10	Conditional	Supporting	Villkor för uppgifter om fällande domar i brottmål och överträdelser
GDPR	Article 24	Controller	Supporting	Personuppgiftsansvarigs ansvar och åtgärder
GDPR	Article 26	Joint Controller	Supporting	Register över arrangemang för gemensamt personuppgiftsansvar
GDPR	Article 28	Both	Supporting	Instruktions- och avtalsregister för personuppgiftsbiträde
GDPR	Article 30	Both	Primary	Register över behandlingsaktiviteter
GDPR	Article 35	Controller	Supporting	Koppling till screening för DPIA
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Ändamålets legitimitet och specificering
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Begränsning av insamling

ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Uppgiftsminimering
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Begränsning av användning, bevarande och utlämnande
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Ansvarsskyldighet
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Kontroller för skydd av PII avseende ändamålets legitimitet, insamling, minimering, användning, bevarande och utlämnande
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Koppling till nytta och utlösare för PIA

1. Omfattning

1.1 Denna policy anger kraven för att upprätthålla PII-behandlingsförteckningen / ROPA och dokumentera rättslig grund, behandlingsändamål, behandlingsroller, kategorier av PII, kategorier av registrerade, mottagare, bevarandereferenser, överföringsreferenser, instruktioner för personuppgiftsbiträde, register för gemensamt personuppgiftsansvar och koppling till screening av integritetsrisker.

1.2 Denna policy gäller för:

1.2.1 alla behandlingsaktiviteter som rör PII inom PIMS-omfattningen;

1.2.2 behandling som utförs som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde eller underbiträde;

1.2.3 behandling som utförs av verksamhetsprocesser, system, applikationer, leverantörer, personuppgiftsbiträden, underbiträden och mottagare vid datadelning;

1.2.4 ny behandling, väsentligt ändrad behandling och avvecklad behandling;

1.2.5 underlag som upprätthålls i REG02 och stödjande underlag i REG01, REG03, REG04, REG05, REG07, REG08, REG09 och REG12.

1.3 Denna policy ersätter inte detaljerade kontroller för integritetsmeddelanden, samtyckeskontroller, metodik för DPIA, genomförande av bevarande, val av mekanism för internationell överföring, avtalskontroller för personuppgiftsbiträden, säkerhetskontroller för PII eller kontroller för dokumenterad information. Dessa krav definieras i de relaterade policyer som anges i avsnitt 12.

1.4 I denna policy avses med en post i behandlingsförteckningen en post i REG02 som beskriver en avgränsad behandlingsaktivitet som rör PII, inklusive dess ändamål, roll, ägare, kategorier av PII, kategorier av registrerade, rättslig grund eller referens till kundinstruktion, system, mottagare, bevarandereferens, överföringsreferens, status för integritetsrisk och granskningsstatus.

1.5 I denna policy avses med en väsentlig behandlingsändring varje ändring av behandlingsändamål, rättslig grund, PIMS-roll, kategori av PII, kategori av registrerade, mottagare, system, leverantör, underbiträde, behandlingsplats, överföring, bevaranderegel, säkerhetsklassificering, integritetsmeddelande, samtyckesberoende, DPIA-status, kundinstruktion eller certifieringsomfattning.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att organisationen kan identifiera, dokumentera, motivera, granska och visa de behandlingsaktiviteter som rör PII inom PIMS-omfattningen.

2.2 Denna policy gör det möjligt för organisationen att upprätthålla en fullständig, aktuell och revisionsklar PII-behandlingsförteckning som stödjer behandling med rättslig grund, ansvarsskyldighet, integritetsmeddelanden, samtyckeshantering, riskbedömning av integritetsrisker, screening för DPIA, bevarande, styrning av överföringar, styrning av personuppgiftsbiträden och PIMS-övervakning.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 fastställa REG02 som den auktoritativa PII-behandlingsförteckningen och bevisobjektet för ROPA;

3.1.2 säkerställa att varje behandlingsaktivitet som rör PII har en ansvarig ägare;

3.1.3 skilja mellan behandlingsposter för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde;

3.1.4 dokumentera specifika behandlingsändamål innan behandlingen påbörjas;

3.1.5 dokumentera rättslig grund för behandling som personuppgiftsansvarig innan behandlingen påbörjas;

3.1.6 dokumentera kundinstruktioner för behandling som personuppgiftsbiträde och underbiträde innan behandlingen påbörjas;

3.1.7 dokumentera kategorier av PII, kategorier av registrerade, mottagare, bevarandereferenser, överföringsreferenser, system och leverantörsrelationer;

3.1.8 koppla poster i förteckningen till underlag för integritetsmeddelande, samtycke, DPIA, risk, leverantör, överföring, kontroll och revision där så är tillämpligt;

3.1.9 säkerställa att poster i behandlingsförteckningen granskas, uppdateras och korrigeras när behandlingen ändras;

3.1.10 undvika att separata register över rättslig grund eller behandlingsförteckningar skapas utanför REG02.

4. Policyuttalanden

4.1 Baslinje för behandlingsförteckning

4.1.1 [Both] Process Owner / Business Owner ska skapa en behandlingsförteckningspost i REG02 innan någon ny behandlingsaktivitet som rör PII påbörjas.

4.1.2 [Both] Process Owner / Business Owner ska registrera de obligatoriska fälten i REG02 för varje behandlingsaktivitet innan aktiviteten påbörjas.

4.1.3 [Both] Privacy Lead / PIMS Manager ska godkänna den obligatoriska fältuppsättningen för REG02 i REG12 före den första PIMS-driften och därefter årligen.

4.1.4 [Both] Process Owner / Business Owner ska klassificera organisationens PIMS-roll för varje behandlingsaktivitet i REG02 innan aktiviteten påbörjas.

4.1.5 [Both] System Owner / Application Owner ska koppla varje system eller applikation som behandlar PII till relevant behandlingsaktivitet i REG02 innan systemet tas i produktion.

4.1.6 [Both] Vendor / Procurement Owner ska koppla varje relation med personuppgiftsbiträde, underbiträde, tredjepartsdelning eller gemensamt personuppgiftsansvar i REG08 till relevant behandlingsaktivitet i REG02 innan avtal godkänns eller onboarding genomförs.

4.2 Register över ändamål och rättslig grund för personuppgiftsansvarig

4.2.1 [Controller] Process Owner / Business Owner ska dokumentera det specifika behandlingsändamålet i REG02 innan PII samlas in, används, lämnas ut eller på annat sätt behandlas.

4.2.2 [Controller] Privacy Lead / PIMS Manager ska validera den rättsliga grund som registrerats i REG02 innan behandling som personuppgiftsansvarig påbörjas och innan någon ändring av ändamål får verkan.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor ska registrera rådgivning i REG12 innan en ny rättslig grund godkänns för högriskbehandling, PII i särskilda kategorier, uppgifter om fällande domar i brottmål eller överträdelser, eller väsentligt ändrad behandling som personuppgiftsansvarig.

4.2.4 [Controller] Process Owner / Business Owner ska koppla REG02 till REG05 innan behandling som personuppgiftsansvarig grundas på samtycke som rättslig grund.

4.2.5 [Controller] Process Owner / Business Owner ska registrera referensen till bedömningen av berättigat intresse i REG04 innan behandling som personuppgiftsansvarig grundas på berättigade intressen.

4.2.6 [Conditional] Process Owner / Business Owner ska registrera villkoret för behandling av särskilda kategorier i REG02 innan PII i särskilda kategorier behandlas.

4.2.7 [Conditional] Privacy Lead / PIMS Manager ska registrera auktorisationsgrunden för uppgifter om fällande domar i brottmål eller överträdelser i REG02 innan sådana uppgifter behandlas.

4.2.8 [Controller] Process Owner / Business Owner ska dokumentera ändamålsförenlighet och screening av integritetsrisker i REG02 och REG04 innan PII används för ett nytt ändamål som inte tidigare har registrerats.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1 Undantag för behandlingsförteckning och rättslig grund

9.1.1 [All] Process Owner / Business Owner ska begära ett undantag i REG12 innan en behandlingsaktivitet som rör PII bedrivs utan ett obligatoriskt fält i REG02, post om rättslig grund, referens till kundinstruktion eller granskningsstatus.

9.1.2 [All] Privacy Lead / PIMS Manager ska bedöma påverkan på integritet, certifiering och drift för varje undantag från behandlingsförteckningen i REG12 inom 10 arbetsdagar efter begäran.

9.1.3 [All] Data Protection Officer / Privacy Advisor ska registrera rådgivning i REG12 innan något undantag godkänns som rör rättslig grund, PII i särskilda kategorier, uppgifter om fällande domar i brottmål eller överträdelser, högriskbehandling, koppling till internationell överföring eller begränsning i kundinstruktion.

9.1.4 [All] Top Management ska godkänna undantag från behandlingsförteckningen som överstiger 30 dagar, påverkar högriskbehandling eller påverkar certifieringsomfattningen i REG12 innan undantaget får verkan.

9.1.5 [All] Privacy Lead / PIMS Manager ska ange ett utgångsdatum som inte överstiger 90 dagar i REG12 för varje godkänt undantag från behandlingsförteckningen före godkännande.

9.1.6 [All] Process Owner / Business Owner ska stänga eller ompröva varje undantag från behandlingsförteckningen i REG12 inom fem arbetsdagar efter utgångsdatumet.

10. Tillämpning

10.1 Tillämpning av krav på behandlingsförteckning och rättslig grund

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera saknat, felaktigt, inaktuellt eller icke godkänt underlag för behandlingsförteckningen i REG02 som en avvikelse i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [Controller] Process Owner / Business Owner ska pausa ny behandling som personuppgiftsansvarig när obligatoriskt underlag för ändamål eller rättslig grund saknas i REG02 före lansering.

10.1.3 [Processor] Process Owner / Business Owner ska pausa ny behandling som personuppgiftsbiträde när obligatoriskt underlag för kundinstruktion saknas i REG02 eller REG08 före onboarding av tjänsten.

10.1.4 [Both] System Owner / Application Owner ska blockera att system tas i produktion för behandling av PII när obligatorisk koppling till förteckningen i REG02 saknas före godkännande av produktionssättning.

10.1.5 [Both] Vendor / Procurement Owner ska blockera onboarding av leverantör, personuppgiftsbiträde, underbiträde, tredjepartsmottagare eller gemensamt personuppgiftsansvar när obligatoriskt kopplingsunderlag i REG02 och REG08 saknas före avtalsgodkännande.

10.1.6 [All] Top Management ska granska olösta större avvikelser som rör behandlingsförteckningen eller rättslig grund i REG12 under ledningens genomgång.

10.1.7 [All] Internal Audit / Compliance Reviewer ska verifiera effektiviteten hos korrigerande åtgärder för avvikelser i behandlingsförteckningen i REG12 vid nästa planerade revision eller inom 60 dagar efter stängning, beroende på vilket som inträffar först.

11. Granskning och underhåll

11.1 Granskning och underhåll av policyn

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy i REG12 årligen och inom 30 dagar efter väsentlig ändring av behandlingsförteckning, rättslig grund, instruktion till personuppgiftsbiträde, ROPA eller certifieringskrav.

11.1.2 [All] Privacy Lead / PIMS Manager ska granska minimikraven på fält i REG02 i REG12 årligen och inom 30 dagar efter väsentlig ändring av rättsliga, regulatoriska, avtalsmässiga eller behandlingsrelaterade krav.

11.1.3 [All] Data Protection Officer / Privacy Advisor ska granska ändringar av denna policy som har betydelse för integritet i REG12 före godkännande.

11.1.4 [All] Top Management ska godkänna väsentliga ändringar av denna policy i REG12 före publicering.

11.1.5 [All] Privacy Lead / PIMS Manager ska uppdatera REG03 och REG04 inom 15 arbetsdagar efter godkända policyändringar som ändrar kontrolltillämplighet eller krav på screening av integritetsrisker.

11.1.6 [All] Privacy Lead / PIMS Manager ska registrera kommunikation av godkända ändringar av denna policy i REG11 inom 30 dagar efter publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII04 - Policy för integritetsmeddelanden och transparens

12.5 PII05 - Policy för hantering av samtycke och preferenser

12.6 PII07 - Policy för riskbedömning av integritetsrisker och DPIA

12.7 PII08 - Policy för integritetsskydd genom design och dataskydd som standard

12.8 PII09 - Policy för insamling, användning, utlämnande och delning av PII

12.9 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.10 PII11 - Policy för riktighet och kvalitet hos PII

12.11 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.12 PII13 - Policy för internationell överföring av PII

12.13 PII14 - Policy för säkerhet och åtkomstkontroll av PII

12.14 PII17 - Policy för dokumenterad information och bevismaterial i PIMS

12.15 PII18 - Policy för övervakning, revision och förbättring av PIMS

13. Referensstandarder och ramverk

13.1 Denna policy är mappad till följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som genomför eller stödjer dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Mappad till fastställande av organisationens PIMS-roll för varje behandlingsaktivitet och åtskillnad mellan sammanhang för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].

13.2.2 **Clause 6.1.2** - Mappad till koppling till utlösare för riskbedömning av integritetsrisker vid nya och väsentligt ändrade behandlingsaktiviteter som rör PII. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].

13.2.3 **Clause 6.1.3** - Mappad till koppling av behandlingsaktiviteter till kontrolltillämplighet och underlag för PIMS Statement of Applicability. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].

13.2.4 **Clause 7.5** - Mappad till upprätthållande av behandlingsförteckning, rättslig grund, instruktioner för personuppgiftsbiträde, granskning, undantag och register över korrigerande åtgärder som styrd dokumenterad information. 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** - Mappad till operativ planering och styrning för att skapa, validera, uppdatera, granska och avveckla poster i behandlingsförteckningen innan behandling påbörjas eller ändras. 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** - Mappad till koppling för operativ riskbedömning av integritetsrisker från poster i behandlingsförteckningen och utlösare vid väsentlig behandlingsändring. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.2.7 **Clause 9.1** - Mappad till övervakning och mätning av behandlingsförteckningens fullständighet, validering av rättslig grund, instruktionskoppling, granskningsstatus, koppling till screening för DPIA och avstämningsundantag. 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** - Mappad till hantering av avvikelser, undantag, korrigerande åtgärder, tillämpning och verifiering av effektivitet för behandlingsförteckningen och rättslig grund. 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** - Mappad till identifiering och dokumentation av behandlingsändamål för personuppgiftsansvarig innan PII samlas in, används, lämnas ut eller på annat sätt behandlas. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].

13.2.10 **Annex A.1.2.3** - Mappad till att fastställa, dokumentera, validera och visa rättslig grund för behandling som personuppgiftsansvarig. 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** - Mappad till screening av nya och väsentligt ändrade behandlingsaktiviteter som personuppgiftsansvarig för behov av DPIA. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].

13.2.12 **Annex A.1.2.8** - Mappad till registrering av behandlingsändamål och referenser till ansvarsfördelning för gemensamt personuppgiftsansvar. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.2.13 **Annex A.1.2.9** - Mappad till upprätthållande av register för personuppgiftsansvarig avseende behandling av PII, inklusive ändamål, kategorier, mottagare, bevarandereferenser, överföringar, rättslig grund, riskscreening, ägare, status och granskningsunderlag. 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** - Mappad till kundavtal och dokumenterat instruktionsunderlag för personuppgiftsbiträde, inklusive föremål, varaktighet, ändamål, kategorier av PII och kategorier av registrerade. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].

13.2.15 **Annex A.2.2.3** - Mappad till att säkerställa att personuppgiftsbiträdets behandlingsändamål förblir förenliga med dokumenterade kundinstruktioner. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].

13.2.16 **Annex A.2.2.7** - Mappad till upprätthållande av register för personuppgiftsbiträde avseende behandling av PII för kunders räkning. 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)** - Mappad till behandlingsändamål för personuppgiftsansvarig, validering av rättslig grund och underlag för ansvarsskyldighet innan behandling påbörjas. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].

13.3.2 **Article 5(1)(b)** - Mappad till ändamålsspecificering, bedömning av ändamålsförenlighet och förhindrande av behandling för nya odokumenterade ändamål. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].

13.3.3 **Article 5(1)(c)** - Mappad till registrering av kategorier av PII, kategorier av registrerade och källdata innan behandling för att stödja granskning av minimering. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.3.4 **Article 5(1)(e)** - Mappad till registrering av bevaranderegel eller bevarandereferens för varje behandlingsaktivitet. Addressed by clauses [4.4.4; 8.1.6].

13.3.5 **Article 5(2)** - Mappad till underlag för ansvarsskyldighet avseende behandlingsförteckning, validering av rättslig grund, granskning, avstämning, revisionsstickprov och korrigerande åtgärder. 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 - Mappad till dokumentation och validering av rättslig grund för behandling som personuppgiftsansvarig, inklusive koppling till samtycke, referens till bedömning av berättigat intresse och ändamålsförenlighet. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].

13.3.7 Article 9 - Mappad till registrering av villkor för behandling av särskilda kategorier och integritetsrådgivning innan behandling av PII i särskilda kategorier. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].

13.3.8 **Article 10** - Mappad till registrering av auktorisationsgrund för uppgifter om fällande domar i brottmål eller överträdelser före behandling. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].

13.3.9 **Article 24** - Mappad till styrning, granskning, ansvarsskyldighet och ledningstillsyn för personuppgiftsansvarig avseende behandlingsförteckning och register över rättslig grund. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].

13.3.10 **Article 26** - Mappad till behandlingsändamål och underlag för ansvarsfördelning för gemensamt personuppgiftsansvar. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].

13.3.11 **Article 28** - Mappad till instruktioner, avtal, relationskoppling och onboardingkontroller för personuppgiftsbiträden och underbiträden. 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** - Mappad till register över behandlingsaktiviteter för personuppgiftsansvariga och personuppgiftsbiträden, inklusive behandlingsändamål, kategorier av PII, kategorier av registrerade, mottagare, överföringar, bevarandereferenser och register över kundinstruktioner. 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** - Mappad till koppling till screening för DPIA vid nya, väsentligt ändrade eller högriskfyllda behandlingsaktiviteter som personuppgiftsansvarig. 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** - Mappad till ändamålets legitimitet, ändamålsspecificering, koppling till rättslig grund och underlag för ändamålsförenlighet. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].

13.4.2 **Clause 5.4** - Mappad till begränsning av insamling genom dokumentation av kategorier av PII, kategorier av registrerade, källor och motivering innan behandling påbörjas. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].

13.4.3 **Clause 5.5** - Mappad till uppgiftsminimering genom krav på förteckningsfält, kategoridokumentation, mottagardokumentation och granskning av aktuella behandlingsposter. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].

13.4.4 **Clause 5.6** - Mappad till begränsning av användning, bevarande, utlämnande och överföring genom dokumenterade ändamål, mottagarkategorier, bevarandereferenser, överföringskoppling och kontroller för ändring av ändamål. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].

13.4.5 **Clause 5.10** - Mappad till ansvarsskyldighet genom ägarskap, styrning av förteckningen, granskning, avstämning, revisionsstickprov, undantagshantering och underlag för korrigerande åtgärder. 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** - Mappad till kontroller för skydd av PII avseende ändamålets legitimitet, begränsning av insamling, uppgiftsminimering och begränsning av användning, bevarande och utlämnande. 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** - Mappad till användning av ändringar i behandlingsförteckningen för att utlösa riskbedömning av integritetsrisker och screening för DPIA innan ny eller väsentligt ändrad behandling fortsätter. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].