					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII07					Dokumenttitel: **Policy för bedömning av integritetsrisker och DPIA**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-risker och möjligheter
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Bedömning av integritetsrisker
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Riskbehandling av integritetsrisker och koppling till SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planerade PIMS-ändringar och förnyad riskbedömning
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterad information om integritetsrisker och DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operativ planering och styrning
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operativ bedömning av integritetsrisker
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operativ riskbehandling av integritetsrisker
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Övervakning och mätning av integritetsrisker
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Ledningens genomgång av integritetsrisker
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Riskrelaterad avvikelse och korrigerande åtgärd
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Konsekvensbedömning avseende integritet
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Behandlingsregister som stöd för riskbedömning
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Kundavtal för personuppgiftsbiträde och stöd vid DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Information från personuppgiftsbiträde som stöd för kundens efterlevnad
GDPR	Article 5(2)	Controller	Supporting	Underlag för ansvarsskyldighet

GDPR	Article 24	Controller	Supporting	Personuppgiftsansvarigs ansvar och åtgärder
GDPR	Article 25	Controller	Supporting	Dataskydd genom design och som standard
GDPR	Article 28	Both	Supporting	Biträdesstöd och instruktioner
GDPR	Article 30	Both	Supporting	Behandlingsregister som stöd för DPIA
GDPR	Article 32	Both	Supporting	Säkerhetsrisk och skyddsåtgärder
GDPR	Article 35	Controller	Primary	Konsekvensbedömning avseende dataskydd
GDPR	Article 36	Controller	Primary	Förhandssamråd
GDPR	Article 39	Conditional	Supporting	DPO-rådgivning och övervakning där det är tillämpligt
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Dataskyddskontroller, informationssäkerhet och efterlevnad av integritetskrav
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA-omfattning, nytta, utlösande faktor och förberedelse
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program för PII-skydd och identifiering av krav
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	Integrering av organisationens hantering av integritetsrisker

1. Omfattning

1.1 Denna policy fastställer kraven för bedömning av integritetsrisker, DPIA-screening, genomförande av fullständig DPIA, riskbehandling, acceptans av kvarstående risk, samråd, granskning och hantering av bevismaterial för behandling av PII inom PIMS-omfattningen.

1.2 Denna policy gäller för:

1.2.1 nya och väsentligt ändrade behandlingsaktiviteter för PII;

1.2.2 behandlingssammanhang för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde;

1.2.3 system, applikationer, tjänster, verksamhetsprocesser, leverantörer, personuppgiftsbiträden, underbiträden, internationella överföringar och upplägg för datadelning som påverkar behandling av PII;

1.2.4 underlag för integritetsrisker och DPIA som underhålls i REG04 samt stödjande underlag som underhålls i REG02, REG03, REG08, REG09, REG10, REG11 och REG12.

1.3 Denna policy ersätter inte kontroller för behandlingsregister, integritetsmeddelanden, samtycke, registrerades rättigheter, inbyggt dataskydd, leverantörer, internationella överföringar, PII-säkerhet, incidenter, dokumenterad information eller övervakning/revision/förbättring. Dessa krav definieras i de relaterade policyer som anges i avsnitt 12.

1.4 I denna policy avses med bedömning av integritetsrisker dokumenterad identifiering, analys, utvärdering, behandling, granskning och övervakning av potentiellt negativa integritetskonsekvenser som uppstår genom behandling av PII.

1.5 I denna policy avses med DPIA en dokumenterad bedömning som används för behandling som personuppgiftsansvarig och som sannolikt leder till hög risk för registrerade samt som utvärderar behandlingens nödvändighet, proportionalitet, risker, skyddsåtgärder, kvarstående risk, behov av samråd och villkor för godkännande.

1.6 I denna policy avses med hög kvarstående integritetsrisk en integritetsrisk som efter föreslagen eller genomförd riskbehandling ligger över den godkända acceptanströskeln.

1.7 I denna policy avses med väsentlig ändring varje ändring som påverkar PIMS-omfattning, behandlingsändamål, rättslig grund, PII-kategorier, kategorier av registrerade, behandlingens omfattning, behandlingsteknik, övervakning eller profilering, automatiserat beslutsfattande, sårbara registrerade, mottagare, personuppgiftsbiträden, underbiträden, internationella överföringar, bevarande, säkerhetskontroller, riskprofil, kundinstruktioner eller certifieringsomfattning.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att integritetsrisker och DPIA-skyldigheter identifieras, bedöms, behandlas, godkänns, granskas och beläggs innan behandling av PII skapar oacceptabel risk för registrerade eller för PIMS.

2.2 Denna policy gör det möjligt för organisationen att visa riskbaserad integritetsstyrning, ansvarsskyldighet för DPIA hos personuppgiftsansvarig, stöd från personuppgiftsbiträde vid DPIA, dokumenterad riskbehandling, godkännande av kvarstående risk, beslutsfattande om förhandssamråd och ständig förbättring av dataskyddskontroller.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 fastställa obligatoriska utlösande faktorer för screening av integritetsrisker;

3.1.2 fastställa när en fullständig DPIA krävs;

3.1.3 säkerställa att DPIA-beslut hos personuppgiftsansvarig dokumenteras och kan granskas;

3.1.4 säkerställa att stöd från personuppgiftsbiträde och underbiträde vid DPIA dokumenteras när det krävs enligt kundinstruktion eller avtal;

3.1.5 säkerställa att integritetsrisker bedöms innan ny eller väsentligt ändrad behandling av PII går vidare;

3.1.6 säkerställa att riskbehandling av integritetsrisker tilldelas, genomförs och verifieras;

3.1.7 säkerställa att höga kvarstående integritetsrisker eskaleras och godkänns innan behandling inleds eller fortsätter;

3.1.8 säkerställa att beslut om förhandssamråd dokumenteras när hög kvarstående risk kvarstår;

3.1.9 säkerställa att underlag för integritetsrisker och DPIA underhålls i REG04 och kopplas till relaterade bevisobjekt;

3.1.10 undvika att skapa separata register för DPIA, risk eller samråd utanför REG04.

4. Policyuttalanden

4.1 Screening av integritetsrisker

4.1.1 [Both] Process Owner / Business Owner ska initiera screening av integritetsrisker i REG04 innan ny eller väsentligt ändrad behandling av PII som registrerats i REG02 inleds.

4.1.2 [Both] Privacy Lead / PIMS Manager ska underhålla kriterier för screening av integritetsrisker i REG04 före första PIMS-drift och därefter årligen.

4.1.3 [Controller] Process Owner / Business Owner ska genomföra DPIA-screening i REG04 innan behandling som personuppgiftsansvarig och som uppfyller kriterierna för screening av integritetsrisker inleds.

4.1.4 [Processor] Vendor / Procurement Owner ska registrera kundens krav på stöd vid DPIA i REG08 innan behandling som personuppgiftsbiträde inleds, när kundavtalet eller dokumenterad instruktion kräver DPIA-stöd.

4.1.5 [Both] System Owner / Application Owner ska tillhandahålla underlag om systemdesign, åtkomst, säkerhet, loggning och dataflöden i REG04 innan bedömning av integritetsrisker godkänns för nya eller väsentligt ändrade system som behandlar PII.

4.1.6 [Both] Privacy Lead / PIMS Manager ska registrera screeningresultatet och motiveringen till beslutet om fullständig DPIA i REG04 innan behandlingsaktiviteten går vidare.

4.2 Utlösande faktorer för DPIA och fastställande av krav

4.2.1 [Controller] Privacy Lead / PIMS Manager ska kräva en fullständig DPIA i REG04 innan behandling som personuppgiftsansvarig och som sannolikt leder till hög risk inleds.

4.2.2 [Controller] Process Owner / Business Owner ska hänskjuta behandling som omfattar storskalighet, systematisk övervakning, profilering, automatiserade beslut, särskilda kategorier av PII, uppgifter om fällande domar eller lagöverträdelser, sårbara registrerade, innovativ teknik eller väsentligt ändrad behandling till Privacy Lead / PIMS Manager i REG04 innan behandlingen inleds.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor ska registrera rådgivning i REG04 innan beslut om krav på fullständig DPIA för behandling med hög risk godkänns.

4.2.4 [Both] Process Owner / Business Owner ska göra förnyad screening av integritetsrisker i REG04 innan PII används för ett nytt ändamål, en ny mottagare läggs till, ett nytt personuppgiftsbiträde eller underbiträde införs, systemarkitekturen ändras eller en ny internationell överföring påbörjas.

4.2.5 [Processor] Privacy Lead / PIMS Manager ska dokumentera huruvida DPIA-stöd från personuppgiftsbiträde krävs i REG08 inom 10 arbetsdagar efter mottagande av en kundbegäran om DPIA-stöd.

4.2.6 [Subprocessor] Vendor / Procurement Owner ska dokumentera uppströms krav på DPIA-stöd i REG08 innan underbiträdesbehandling inleds, när det uppströms kundavtalet eller personuppgiftsbiträdesavtalet kräver sådant stöd.

[... 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 avseende integritetsrisker och DPIA

9.1.1 [All] Process Owner / Business Owner ska begära varje undantag från denna policy i REG12 innan avvikelsen sker.

9.1.2 [All] Privacy Lead / PIMS Manager ska bedöma den integritetsmässiga, rättsliga, certifieringsmässiga, operativa och registrerades påverkan av varje begärt undantag i REG04 eller REG12 inom 10 arbetsdagar efter begäran.

9.1.3 [All] Data Protection Officer / Privacy Advisor ska registrera rådgivning i REG12 innan godkännande av varje undantag som påverkar behandling med hög risk, slutförande av fullständig DPIA, förhandssamråd, hög kvarstående integritetsrisk eller kundens DPIA-stöd.

9.1.4 [All] Top Management ska godkänna undantag avseende integritetsrisk eller DPIA som påverkar behandling med hög risk, certifieringsomfattning, förhandssamråd eller olöst hög kvarstående integritetsrisk 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 avseende integritetsrisk eller DPIA före godkännande.

9.1.6 [All] Process Owner / Business Owner ska stänga eller ompröva varje undantag avseende integritetsrisk eller DPIA i REG12 inom fem arbetsdagar efter utgång.

10. Tillämpning

10.1 Tillämpning av integritetsrisk- och DPIA-krav

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera saknat, felaktigt, ofullständigt, försenat eller ej godkänt underlag för integritetsrisk eller DPIA i REG04 som en avvikelse i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [Controller] Process Owner / Business Owner ska avbryta ny behandling med hög risk som personuppgiftsansvarig när erforderligt underlag för DPIA-godkännande i REG04 saknas före lansering.

10.1.3 [Both] System Owner / Application Owner ska blockera att system som behandlar PII tas i produktion när erforderligt underlag för riskbehandling i REG04 saknas före godkännande att tas i produktion.

10.1.4 [Both] Vendor / Procurement Owner ska blockera onboarding av leverantör, personuppgiftsbiträde, underbiträde eller datadelning när erforderligt underlag för integritetsrisk eller DPIA-stöd i REG04 saknas före avtalsgodkännande.

10.1.5 [All] Top Management ska granska olösta större avvikelser avseende integritetsrisk eller DPIA i REG12 vid ledningens genomgång.

10.1.6 [All] Privacy Lead / PIMS Manager ska eskalera upprepade missade tidsfrister för screening i REG04, DPIA-granskning eller riskbehandling till Top Management i REG12 inom fem arbetsdagar efter den andra förekomsten under en 12-månadersperiod.

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

11. Granskning och underhåll

11.1 Policygranskning och underhåll

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy i REG12 årligen och inom 30 dagar efter väsentlig ändring av krav avseende integritetsrisk, DPIA, förhandssamråd, biträdesstöd eller certifiering.

11.1.2 [All] Privacy Lead / PIMS Manager ska årligen granska screeningkriterier i REG04, kriterier för DPIA-utlösande faktorer, riskklassningskriterier och kriterier för acceptans av kvarstående risk i REG12.

11.1.3 [All] Data Protection Officer / Privacy Advisor ska granska ändringar av denna policy som är betydande för integritetsskyddet 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, riskkriterier eller krav på DPIA-screening.

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 PII03 - Policy för behandlingsregister avseende PII och rättslig grund

12.5 PII04 - Policy för integritetsmeddelanden och transparens

12.6 PII05 - Policy för hantering av samtycke och preferenser

12.7 PII06 - Policy för hantering av registrerades rättigheter

12.8 PII08 - Policy för inbyggt dataskydd och dataskydd som standard

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

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

12.11 PII11 - Policy för korrekthet och kvalitet i PII

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

12.13 PII13 - Policy för internationell överföring av PII

12.14 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.15 PII15 - Policy för hantering av PII-incidenter och personuppgiftsincidenter

12.16 PII17 - Policy för dokumenterad information och bevismaterial i PIMS

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

13. Referensstandarder och ramverk

13.1 Denna policy är mappad mot 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 6.1.1** - Mappad till identifiering och planering av åtgärder för integritetsrisker och möjligheter med hjälp av screeningkriterier, risktrösklar, eskalering och indata till ledningens genomgång. 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** - Mappad till genomförande av screening av integritetsrisker, bedömning av integritetsrisker, riskklassning, förnyad bedömning och utvärdering av DPIA-utlösande faktorer innan ny eller väsentligt ändrad behandling går vidare. 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** - Mappad till planering av riskbehandling av integritetsrisker, uppdatering av kontrolltillämplighet, genomförande av behandling, acceptans av kvarstående risk och koppling till SoA. 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** - Mappad till planerade PIMS- och behandlingsändringar som utlöser förnyad bedömning av integritetsrisker och DPIA-granskning. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mappad till styrd dokumenterad information för screening av integritetsrisker, DPIA-underlag, riskbehandling, acceptans av kvarstående risk, beslut om förhandssamråd, undantag, avvikelser och underlag för policygranskning. 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** - Mappad till drift av kontroller för integritetsrisker och DPIA före tas i produktion, onboarding, behandlingsgodkännande, stängning av behandlingsåtgärder och koppling till korrigerande åtgärder. 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** - Mappad till operativ bedömning av integritetsrisker för nya, ändrade, systemrelaterade, leverantörsrelaterade, överföringsrelaterade och incidentdrivna förändringar av behandling. 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** - Mappad till operativ riskbehandling av integritetsrisker, tilldelning av behandling, genomförande av behandling, eskalering av försenad behandling och verifiering av effektivitet. 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** - Mappad till övervakning och mätning av screeningtäckning, DPIA-status, öppna risker, försenade behandlingsåtgärder, leverantörsåtgärder, säkerhetsbehandlingsåtgärder, incidentbaserade omprövningsåtgärder och revisionsiakttagelser. 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** - Mappad till ledningens genomgång av höga kvarstående integritetsrisker, försenade behandlingsåtgärder, status för fullständig DPIA, beslut om förhandssamråd och större undantag avseende integritetsrisk. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mappad till avvikelser avseende integritetsrisker och DPIA, undantag, öppnande av korrigerande åtgärder, eskalering och verifiering av effektivitet. 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** - Mappad till bedömning av behovet av, och där det är lämpligt genomförande av, konsekvensbedömning avseende integritet för ny eller ändrad behandling som personuppgiftsansvarig. 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** - Mappad till behandlingsregister som stödjer indata för bedömning av integritetsrisker och DPIA, inklusive ändamål, kategorier, system, mottagare, överföringar och leverantörer. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mappad till kundavtal för personuppgiftsbiträde och skyldigheter avseende DPIA-stöd till kund. 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** - Mappad till personuppgiftsbiträdets tillhandahållande av information som behövs för kundens efterlevnad, inklusive DPIA-stöd och underlag för kundstöd. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappad till underlag för ansvarsskyldighet avseende DPIA-screening, beslut om fullständig DPIA, riskbehandling, acceptans av kvarstående risk, beslut om

förhandssamråd, undantag, revisionsiakttagelser och korrigerande åtgärder. 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** - Mappad till personuppgiftsansvarigs ansvar för lämpliga åtgärder avseende integritetsrisker, granskning av hög kvarstående risk, ledningens godkännande och policyunderhåll. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mappad till underlag för integritetsskydd genom design och dataskydd som standard som används vid riskbedömning och före godkännande att tas i produktion. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mappad till DPIA-stöd från personuppgiftsbiträden och underbiträden, hantering av kundinstruktioner och underlag för leverantörsriskbehandling. 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** - Mappad till behandlingsregister som stödjer indata till bedömning av integritetsrisker och DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mappad till indata om PII-säkerhetsrisker, val av skyddsåtgärder, behandling av säkerhetsrisker och uppdateringar av status för säkerhetskontroller. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mappad till DPIA-screening, fastställande av krav på fullständig DPIA, DPIA-innehåll, DPO-rådgivning, granskning och blockering av behandling med hög risk utan erforderligt DPIA-godkännande. 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** - Mappad till beslutsfattande om förhandssamråd, DPO-rådgivning, godkännande av Top Management samt åtgärder för fortsättning, avbrytande, omdesign eller samråd när hög kvarstående risk kvarstår. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mappad till rådgivning och övervakning från Data Protection Officer / Privacy Advisor där det är tillämpligt för DPIA-beslut, behandling med hög risk, förhandssamråd och policyändringar. 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** - Mappad till identifiering av dataskyddskontroller, säkerhetsåtgärder, efterlevnad av integritetskrav, underlag för integritetsrisker, övervakning och granskning. 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** - Mappad till PIA-processens omfattning, nytta, fastställande av utlösande faktor, förberedelse, bedömningsindata, intressentunderlag och DPIA-rapportstruktur som underhålls i REG04. 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** - Mappad till krav på program för PII-skydd, identifiering av krav på PII-skydd, riskbaserat urval av kontroller och koppling till riskbehandling av integritetsrisker. 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** - Mappad till organisationens principer för integritetsrisker, ledarskap, integrering, riskbedömning, riskbehandling, övervakning och granskning samt registrering och rapportering. 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].