					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII09					Dokumenttitel: **Policy för insamling, användning, utlämnande och delning av PII**							
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 7.5; Clause 8.1	Both	Primary	Dokumenterad operativ styrning
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Ändamål och behandlingsregister
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Koppling till rättslig grund
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Ansvar för delning mellan gemensamt personuppgiftsansvariga
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Begränsningar för insamling, behandling och minimering
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Koppling till dirigering av överföring
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Register över överföringar och utlämnanden
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Instruktioner och register för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Koppling till dirigering av överföring för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Register och begäranden avseende utlämnande från personuppgiftsbiträde
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Ändamålsbegränsning, uppgiftsminimering och ansvarsskyldighet
GDPR	Article 6	Controller	Referenced	Koppling till rättslig grund
GDPR	Article 24	Controller	Supporting	Den personuppgiftsansvariges ansvar
GDPR	Article 26	Joint Controller	Supporting	Arrangemang för gemensamt personuppgiftsansvariga
GDPR	Article 28	Both	Supporting	Instruktioner till personuppgiftsbiträden

				och begränsningar för utlämnande
GDPR	Article 30	Both	Supporting	Register över behandling och mottagare
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Ändamåls-, insamlings-, minimerings- och utlämnandebegränsning
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Ansvarsskyldighet och efterlevnad av integritetskrav
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Kontroller för ändamål, insamling, minimering, användning och utlämnande

1. Omfattning

1.1 Denna policy anger krav för insamling, användning, utlämnande och delning av PII inom PIMS-omfattningen.

1.2 Denna policy gäller för:

1.2.1 insamling av PII via direkta, indirekta, automatiserade, manuella, interna, externa och tredjepartskanaler;

1.2.2 godkänd intern användning av PII i verksamhetsprocesser, system och applikationer;

1.2.3 sekundär användning av PII för ett nytt eller väsentligt ändrat ändamål;

1.2.4 externt utlämnande av PII till mottagare, partner, myndigheter, personuppgiftsbiträden, underbiträden, leverantörer och andra tredje parter;

1.2.5 återkommande upplägg för datadelning och engångsutlämnanden;

1.2.6 sammanhang som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde;

1.2.7 REG02 - PII Processing Inventory / ROPA, REG08 - Processor, Subprocessor and Data Sharing Register, REG09 - International Transfer Register och REG12 - Audit, Nonconformity, Corrective Action and Improvement Register.

1.3 Denna policy ersätter inte:

1.3.1 PII03 avseende behandlingsregister, rättslig grund och ägarskap för ROPA;

1.3.2 PII04 avseende innehåll i integritetsmeddelanden, publicering och versionshantering;

1.3.3 PII05 avseende drift av samtycke och preferenser;

1.3.4 PII06 avseende hantering av rättighetsbegäranden från registrerade;

1.3.5 PII07 avseende DPIA-metodik och bedömning av integritetsrisker;

1.3.6 PII08 avseende grindar för inbyggt dataskydd;

1.3.7 PII10 avseende genomförande av bevarande, radering och bortskaffning;

1.3.8 PII11 avseende hantering av riktighet och kvalitet;

1.3.9 PII12 avseende livscykelstyrning för personuppgiftsbiträden, underbiträden och tredje parter;

1.3.10 PII13 avseende val av mekanism för internationell överföring och riskkontroller för överföring;

1.3.11 PII14 avseende PII-säkerhet och åtkomstkontroll;

1.3.12 PII15 avseende incident- och personuppgiftsincidenthantering;

1.3.13 PII18 avseende PIMS-övergripande styrning av övervakning, revision, avvikelse, korrigerande åtgärder och förbättring.

1.4 I denna policy gäller följande:

1.4.1 ”godkänd användning” avser en användning av PII som är registrerad i REG02 för en specifik behandlingsaktivitet, ett specifikt ändamål, en PII-kategori, en kategori av registrerade, verksamhetsägare och tillämplig PIMS-roll.

1.4.2 ”insamling” avser att inhämta PII direkt från en registrerad, indirekt från en annan part, automatiskt från ett system eller en enhet, eller via en intern eller extern datakälla.

1.4.3 ”sekundär användning” avser användning av PII för ett ändamål som inte redan är registrerat som ett godkänt ändamål i REG02 för den relevanta behandlingsaktiviteten.

1.4.4 ”förenlighetsbedömning” avser en dokumenterad bedömning i REG02 av det ursprungliga ändamålet, det föreslagna ändamålet, beroendet av rättslig grund, PII-kategorier, de

registrerades förväntningar, minimeringsmotivering, påverkan på utlämnande eller överföring samt hänvisning till andra PIMS-policyer vid behov.

1.4.5 ”externt utlämnande” avser att göra PII tillgänglig för en part utanför organisationen eller utanför den dokumenterade kedjan för kundinstruktioner.

1.4.6 ”datadelning” avser ett återkommande eller strukturerat upplägg enligt vilket PII lämnas ut, överförs, görs åtkomlig, utbyts eller görs tillgänglig för en annan part.

1.4.7 ”återkommande delning av känsliga personuppgifter” avser återkommande delning som omfattar PII av särskilda kategorier, PII om brott, barns PII, register med stor påverkan, storskalig delning eller extern delning som omfattar en överföringsplats som är registrerad i REG09.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att PII samlas in, används, lämnas ut och delas endast för dokumenterade, godkända, begränsade och ansvarsskyldiga ändamål.

2.2 Denna policy gör det möjligt för organisationen att visa att insamling och användning är kopplade till behandlingsposter i REG02, att utlämnanden och upplägg för datadelning registreras i REG08, att dirigering av internationella överföringar är kopplad till REG09 och att undantag och avvikelser hanteras genom REG12.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 begränsa insamling till PII som är nödvändig för dokumenterade ändamål;

3.1.2 säkerställa att intern användning av PII godkänns innan behandlingen påbörjas;

3.1.3 kräva förenlighetsbedömningar före sekundär användning;

3.1.4 kräva godkännande och underlag före externt utlämnande;

3.1.5 upprätthålla underlag för datadelning i REG08 utan att skapa ett separat register för datadelning;

3.1.6 dirigera beroenden av internationella överföringar till REG09 och PII13 utan att duplicera kontroller för överföringsmekanismer;

3.1.7 definiera granskningsintervall för återkommande delning;

3.1.8 upprätthålla underlag med beredskap för revision avseende insamling, användning, utlämnande, delning, undantag och korrigerande åtgärder.

4. Policyuttalanden

4.1 Begränsning av insamling

4.1.1 [Controller] The Process Owner / Business Owner MUST registrera insamlingsändamål, källa eller kanal, PII-kategorier, kategorier av registrerade och minsta dataelement i REG02 innan någon ny insamlingsaktivitet eller väsentlig ändring av insamling påbörjas.

4.1.2 [Controller] The Privacy Lead / PIMS Manager MUST granska insamlingsposten i REG02 innan insamling påbörjas när en ny PII-kategori, källa, kanal eller ett nytt ändamål läggs till.

4.1.3 [Controller] The Process Owner / Business Owner MUST registrera en nödvändighetsmotivering i REG02 för varje PII-dataelement innan elementet samlas in.

4.1.4 [Processor] The Process Owner / Business Owner MUST registrera kundinstruktionsreferensen från REG08 i REG02 innan PII samlas in för en kunds räkning.

4.1.5 [Joint Controller] The Process Owner / Business Owner MUST registrera ansvarsfördelningen för insamling mellan gemensamt personuppgiftsansvariga i REG08 innan gemensam insamling påbörjas.

4.2 Kontroller för godkänd intern användning

4.2.1 [Controller] The Process Owner / Business Owner MUST registrera regler för godkänd intern användning för varje behandlingsaktivitet i REG02 innan användningen påbörjas.

4.2.2 [Controller] The System Owner / Application Owner MUST endast införa arbetsflödesfält, rapporter eller exporter för intern användning som har en motsvarande regel för godkänd användning i REG02 innan produktionssättning.

4.2.3 [Processor] The Process Owner / Business Owner MUST registrera överensstämmelse med kundinstruktioner i REG08 innan kundens PII används för någon aktivitet som personuppgiftsbiträde eller underbiträde.

4.2.4 [Controller] The Privacy Lead / PIMS Manager MUST granska regler för godkänd användning i REG02 minst årligen för varje aktiv behandlingsaktivitet.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST registrera en avvikelse i REG12 inom fem arbetsdagar när odokumenterad intern användning av PII identifieras.

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

9. Undantag

9.1.1 [All] The Process Owner / Business Owner MUST registrera en undantagsbegäran i REG12 innan avvikelse från en godkänd regel för insamling, användning, utlämnande eller delning sker.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST registrera ett beslut om godkännande eller avslag i REG12 innan ett undantag aktiveras.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST registrera rådgivning i REG12 innan godkännande av ett undantag som omfattar oförenlig sekundär användning, återkommande delning av känsliga personuppgifter, konflikt avseende rättsligt bindande utlämnande eller dirigering av överföring.

9.1.4 [All] Top Management MUST registrera godkännande i REG12 innan aktivering av något undantag med en varaktighet som överstiger 30 kalenderdagar eller påverkar mer än en behandlingsaktivitet.

9.1.5 [All] The Process Owner / Business Owner MUST stänga ett undantag i REG12 senast på utgångsdatumet eller inom fem arbetsdagar efter att undantagsvillkoret upphör.

10. Tillämpning

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registrera icke godkänd insamling, användning, utlämnande eller delning som en avvikelse i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [Controller] The Process Owner / Business Owner MUST stoppa insamling, användning, utlämnande eller delning inom en arbetsdag när Privacy Lead / PIMS Manager registrerar avsaknad av godkänt underlag i REG02 eller REG08 i REG12.

10.1.3 [Processor] The Process Owner / Business Owner MUST registrera ett beslut om stopp eller eskalering i REG08 och REG12 inom en arbetsdag när kundens PII används eller lämnas ut utanför dokumenterad instruktion.

10.1.4 [All] Top Management MUST granska olösta avvikelser med stor påverkan avseende insamling, användning, utlämnande eller delning i REG12 inom 30 kalenderdagar efter eskalering.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST verifiera underlag för stängning av korrigerande åtgärd i REG12 inom 15 arbetsdagar efter att Privacy Lead / PIMS Manager markerar stängning.

11. Granskning och underhåll

11.1.1 [All] The Privacy Lead / PIMS Manager MUST granska denna policy minst årligen och registrera beslutet i REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST granska denna policy inom 30 kalenderdagar efter en väsentlig ändring av PIMS-omfattning, behandlingsändamål, delningsmodell, dirigering av överföringar eller tillämplig skyldighet och registrera utfallet i REG12.

11.1.3 [All] The Process Owner / Business Owner MUST omcertifiera aktiva poster i REG02 och REG08 minst årligen och inom 30 kalenderdagar efter en väsentlig behandlingsändring.

11.1.4 [All] The Internal Audit / Compliance Reviewer MUST inkludera PII09-kontroller i årligt revisionsurval och registrera täckning i REG12.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST uppdatera referenser till relaterade policyer i REG12 inom tio arbetsdagar när PII03, PII08, PII10, PII12, PII13, PII14 eller PII18 ändrar denna policys operativa gräns.

12. Relaterade policyer

12.1 Denna policy bör läsas tillsammans med:

12.1.1 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.1.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.1.3 PII03 - Policy för PII-behandlingsregister och rättslig grund

12.1.4 PII04 - Policy för integritetsmeddelanden och transparens

12.1.5 PII05 - Policy för samtyckes- och preferenshantering

12.1.6 PII06 - Policy för hantering av registrerades rättigheter

12.1.7 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.1.8 PII08 - Policy för inbyggt dataskydd och dataskydd som standard

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

12.1.10 PII11 - Policy för riktighet och kvalitet i PII

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

12.1.12 PII13 - Policy för internationella PII-överföringar

12.1.13 PII14 - Policy för PII-säkerhet och åtkomstkontroll

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

12.1.15 PII17 - Policy för dokumenterad information och bevismaterial i PIMS

12.1.16 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 7.5; Clause 8.1** - Mappad mot dokumenterade operativa poster och kontroll över underlag för insamling, godkänd användning, sekundär användning, utlämnande, delning och dirigering av överföringar. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mappad mot övervakning, mätning, granskning, undantagshantering, avvikelse och korrigerande åtgärd för kontroller av insamling, användning, utlämnande och delning. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mappad mot dokumenterade ändamål för personuppgiftsansvariga, poster över godkänd användning och behandlingsunderlag i REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mappad mot koppling till rättslig grund för insamling, användning och dirigering av sekundär användning utan att ersätta PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mappad mot underlag i REG08 för ansvar för insamling och delning mellan gemensamt personuppgiftsansvariga. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mappad mot begränsning av insamling, begränsning av behandling och minimeringsmotivering innan PII samlas in eller används. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mappad mot koppling till dirigering av överföringar genom REG09 utan att ersätta PII13:s kontroller för överföringsmekanismer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mappad mot poster över överföringar, utlämnanden och återkommande upplägg för datadelning i REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mappad mot anpassning till kundinstruktioner för personuppgiftsbiträden samt personuppgiftsbiträdesposter avseende gränser för insamling, användning och sekundär användning. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mappad mot koppling till dirigering av överföringar för personuppgiftsbiträden genom REG09 utan att ersätta PII13:s kontroller för överföringsmekanismer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mappad mot register över utlämnande från personuppgiftsbiträden, status för avisering vid begäran om utlämnande och underlag för godkännande av utlämnande i REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mappad mot underlag för ändamålsbegränsning, uppgiftsminimering och ansvarsskyldighet avseende insamling, användning, sekundär användning, utlämnande och delning. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mappad mot koppling till rättslig grund och dirigering för ny eller oförenlig sekundär användning utan att ersätta PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mappad mot styrning för personuppgiftsansvariga, godkännanden, granskning och ansvarsskyldighetsåtgärder för insamling, användning, utlämnande och delning. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mappad mot underlag för ansvar för insamling och delning mellan gemensamt personuppgiftsansvariga. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mappad mot instruktioner för personuppgiftsbiträden och underbiträden, kundgodkännande och begränsningar av utlämnande. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mappad mot register över behandling, mottagare, utlämnande och delning i REG02 och REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mappad mot ändamålsspecificering, begränsning av insamling, uppgiftsminimering, begränsning av användning och begränsning av utlämnande. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mappad mot ansvarsskyldighet, underlag för efterlevnad, granskning, undantagshantering, revisionsurval och korrigerande åtgärd. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mappad mot ändamål, begränsning av insamling, minimering, begränsning av användning, begränsning av utlämnande och stöd för register över utlämnande. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].