					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII21					Dokumenttitel: **Integritetspolicy för AI och automatiserat beslutsfattande**							
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 information och operativ styrning för behandlingsunderlag avseende AI, profilering och automatiserat beslutsfattande
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning, avvikelse och korrigerande åtgärder för dataskyddskontroller för AI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Ändamål, rättslig grund, konsekvensbedömning avseende dataskydd och personuppgiftsansvarigs register
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Personuppgiftsbiträdesavtal och ansvar för gemensamt personuppgiftsansvariga vid AI-relaterad behandling av PII
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Skyldigheter gentemot registrerade och transparens för AI-relaterad behandling
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Invändning, åtkomst, rättelse, radering, hantering av begäranden och skyldigheter vid automatiserat beslutsfattande
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 av AI-indata, AI-utdata och härledda data
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Ruttning av internationella överföringar, utlämnanden och begäranden om utlämnande av AI-relaterad PII
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Personuppgiftsbiträdesavtal, dokumenterade instruktioner, stöd för kundens skyldigheter och register

ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Personuppgiftsbiträdets stöd för skyldigheter gentemot registrerade, ruttning av överföringar och hantering av utlämnanden
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Skydd av register och loggning kopplad till AI-relaterad behandling av PII
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profilering, rättvisa, transparens, ändamålsbegränsning, minimering, korrekthet och ansvarsskyldighet
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Laglighet, särskilda kategorier av personuppgifter och skyddsåtgärder för uppgifter om fällande domar eller överträdelser
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Tydlig information, åtkomst och meningsfull information om automatiserat beslutsfattande
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Rättelse, radering, begränsning, invändning och rättigheter vid automatiserat beslutsfattande
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Personuppgiftsansvarigs ansvar, inbyggt dataskydd och dataskydd som standard, gemensamt personuppgiftsansvariga, personuppgiftsbiträden, register, säkerhet, DPIA och DPO-uppgifter
GDPR	Article 44	Conditional	Referenced	Ruttning av internationella överföringar vid AI-relaterad behandling av PII
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Principer för ändamål, insamling, minimering, användning, bevarande, utlämnande, korrekthet och kvalitet
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9;	Both	Supporting	Transparens, individens deltagande,

	Clause 5.10; Clause 5.11; Clause 5.12			ansvarsskyldighet, informationssäkerhet och efterlevnad av dataskyddskrav
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Nytta med PIA, tröskelbedömning och förberedelse för bedömning av AI-relaterade integritetsrisker
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Kontroller för ändamål, insamling, minimering, användning, bevarande, utlämnande, korrekthet och registrerades deltagande

1. Omfattning

1.1 Denna policy fastställer obligatoriska dataskyddskrav för artificiell intelligens, profilering, poängsättning, rekommendationer, beslutsstöd och automatiserat beslutsfattande som använder, härleder, genererar, lämnar ut eller på annat sätt behandlar PII inom PIMS-omfattningen.

1.2 Denna policy gäller för:

1.2.1 AI-aktiverade system, applikationer, modeller, tjänster, arbetsflöden, beslutsmotorer, poängsättningsverktyg, rekommendationssystem, analysmodeller och processer för automatiserat beslutsfattande som behandlar PII;

1.2.2 profilering, segmentering, klassificering, prediktion, inferens, personalisering, rangordning, behörighets- eller kvalificeringsbedömning, bedrägeridetektering, riskpoängsättning, åtkomstbeslut, bedömning kopplad till anställning, barnrelaterad profilering, marknadspersonalisering och liknande behandling där PII ingår;

1.2.3 AI-relaterad PII som används för träning, testning, validering, finjustering, övervakning, produktionsinferens, granskning av utdata, prestationsmätning, incidentutredning eller modellavveckling;

1.2.4 sammanhang där organisationen agerar som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde eller underbiträde;

1.2.5 AI-relaterade leverantörer, personuppgiftsbiträden, underbiträden, mottagare i upplägg för datadelning och rutter för internationell överföring som behandlar PII.

1.3 Denna policy skapar inte ett fullständigt ramverk för AI-styrning, ett ledningssystem för AI, en AI-förteckning, en modellförteckning, ett modellriskregister, ett register för rättvisa, ett algoritmregister, ett AI-incidentregister, en AI-kommitté, en roll som modellägare, en roll som AI-systemägare, ett arbetsflöde för juridisk rådgivning eller ett separat formulär för AI-godkännande.

1.4 Denna policy ersätter inte:

1.4.1 PII03 för behandlingsförteckning, rättslig grund och ägarskap för ROPA;

1.4.2 PII04 för styrning av integritetsmeddelanden;

1.4.3 PII05 för hantering av samtycke och preferenser;

1.4.4 PII06 för arbetsflöde för registrerades rättigheter;

1.4.5 PII07 för metodik för bedömning av integritetsrisker och DPIA;

1.4.6 PII08 för grindar för integritetsskydd genom design och dataskydd som standard;

1.4.7 PII09 för kontroller av insamling, användning, utlämnande och delning;

1.4.8 PII10 för genomförande av bevarande, radering och bortskaffning;

1.4.9 PII11 för kontroller av korrekthet och kvalitet;

1.4.10 PII12 för livscykelstyrning av personuppgiftsbiträden, underbiträden och tredje parter;

1.4.11 PII13 för kontroller av internationella överföringar;

1.4.12 PII14 för säkerhet och åtkomstkontroll;

1.4.13 PII15 för hantering av incidenter och personuppgiftsincidenter;

1.4.14 PII18 för övervakning, revision och förbättring;

1.4.15 PII19 för anställdas integritet;

1.4.16 PII20 för barns integritet;

1.4.17 PII22 för marknadsföringsintegritet och cookies.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att AI, profilering och automatiserat beslutsfattande som involverar PII identifieras, dokumenteras, riskbedöms, är transparenta, kan bestridas, övervakas och styrs genom PIMS utan att skapa dubblerade AI-specifika styrningsartefakter.

2.2 Denna policy säkerställer att integritetsskyldigheter för AI-relaterad behandling av PII styrks genom REG02, REG04, REG06, REG07, REG08, REG09, REG10 och REG12.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 identifiera behandling som involverar PII i AI, profilering och automatiserat beslutsfattande i REG02;

3.1.2 dokumentera AI-relaterade ändamål, rättslig grund, PII-kategorier, datakällor, härledda uppgifter, utdata, mottagare och beslutseffekter i REG02;

3.1.3 utlösa screening av integritetsrisker och ruttning av DPIA genom REG04;

3.1.4 säkerställa att AI-relaterade integritetsmeddelanden och meningsfull information registreras i REG07;

3.1.5 rutta rättighetsbegäranden, invändningar, mänsklig granskning och begäranden om möjlighet att bestrida genom REG06;

3.1.6 styra AI-relaterade personuppgiftsbiträden, underbiträden, leverantörer och upplägg för datadelning genom REG08;

3.1.7 rutta AI-relaterade internationella överföringar genom REG09;

3.1.8 eskalera misstänkta AI-relaterade PII-incidenter, missbruk, obehörigt röjande och negativa integritetsutfall genom REG10 och REG12;

3.1.9 registrera övervakning, undantag, avvikelser, korrigerande åtgärder och förbättringar i REG12.

4. Policyuttalanden

4.1 Identifiering av AI, profilering och automatiserat beslutsfattande

4.1.1 [Controller] När ett nytt eller väsentligt ändrat system, en applikation, modell, ett arbetsflöde, en tjänst eller en verksamhetsprocess föreslås ska Process Owner / Business Owner fastställa om det använder AI, profilering, poängsättning, rekommendationer, beslutsstöd eller automatiserat beslutsfattande som involverar PII och registrera bedömningen i REG02.

4.1.2 [Controller] Innan AI-relaterad behandling av PII påbörjas ska Process Owner / Business Owner dokumentera behandlingsändamål, PII-kategorier, kategorier av registrerade, datakällor, kategorier av härledda data, kategorier av utdata, mottagarkategorier, rättslig grund och bevarandekoppling i REG02.

4.1.3 [Controller] Innan profilering, poängsättning, rekommendationer, beslutsstöd eller automatiserat beslutsfattande används i produktion ska Process Owner / Business Owner dokumentera beslutssammanhanget, den förväntade effekten på registrerade, mänsklig medverkan och rättighetsrutt i REG02 och REG04.

4.1.4 [Joint Controller] Innan AI-relaterad behandling av PII utförs tillsammans med en gemensamt personuppgiftsansvarig ska Privacy Lead / PIMS Manager dokumentera ansvar för fastställande av ändamål, meddelande, rättighetshantering, DPIA-stöd, styrning av personuppgiftsbiträden och incidenteskalering i REG08.

4.1.5 [Processor] Innan PII behandlas genom en AI-relaterad tjänst för en kund ska Process Owner / Business Owner bekräfta att kundinstruktioner, tillåtna ändamål, förbjuden användning, hantering av utdata och skyldigheter att bistå dokumenteras i REG08.

4.1.6 [Both] Innan AI-relaterad behandling av PII aktiveras ska Privacy Lead / PIMS Manager bekräfta att behandlingen är kopplad till tillämpliga kanoniska underlagsobjekt och att inget separat AI-specifikt register skapas utanför REG02, REG04, REG06, REG07, REG08, REG09, REG10 eller REG12.

4.2 Bedömning av integritetsrisker och ruttning av DPIA

4.2.1 [Controller] Innan AI-relaterad behandling av PII lanseras eller ändras väsentligt ska Privacy Lead / PIMS Manager slutföra screening av integritetsrisker och registrera DPIA-beslutet i REG04.

4.2.2 [Conditional] När AI-relaterad behandling innefattar profilering, automatiserade beslut, storskalig utvärdering, särskilda kategorier av personuppgifter, uppgifter om brott, sårbara registrerade, bedömning av anställda, barn, beteendeövervakning, lokaliseringsuppgifter, biometriska uppgifter, poängsättning med hög påverkan eller betydande effekter ska Data Protection Officer / Privacy Advisor granska integritetsrisken och registrera rådgivningen i REG04.

4.2.3 [Controller] Innan AI-relaterad behandling av PII tas i produktion ska Process Owner / Business Owner dokumentera riskbehandlingsåtgärder, status för kvarstående risk och underlag för produktionsberedskap i REG04 eller REG12.

4.2.4 [Controller] Innan PII återanvänds för AI-träning, testning, validering, finjustering, övervakning eller modellförbättring för ett nytt eller väsentligt ändrat ändamål ska Process Owner / Business Owner slutföra integritetsgranskning och registrera beslutet i REG02 och REG04.

4.2.5 [Conditional] När kvarstående integritetsrisk förblir hög efter planerad behandling ska Top Management godkänna, avvisa eller kräva ytterligare behandling före produktionsanvändning och registrera beslutet i REG04 och REG12.

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

9. Undantag

9.1 [All] Innan avvikelse från ett AI-relaterat integritetskrav i denna policy sker ska den begärande Process Owner / Business Owner lämna en undantagsmotivering och underlag för kompenserande kontroller i REG12.

9.2 [Conditional] När ett undantag påverkar profilering, automatiserat beslutsfattande, mänsklig granskning, möjlighet att bestrida, transparens, DPIA-resultat, poängsättning med hög påverkan, barnrelaterad behandling, anställningsrelaterad behandling, begränsningar för personuppgiftsbiträden eller internationella överföringar ska Data Protection Officer / Privacy Advisor granska undantaget och registrera rådgivningen i REG04 eller REG12.

9.3 [Conditional] När ett undantag skapar eller bevarar hög kvarstående integritetsrisk ska Top Management godkänna eller avvisa undantaget och registrera beslutet i REG04 och REG12.

9.4 [All] Innan ett godkänt AI-relaterat integritetsundantag löper ut ska Privacy Lead / PIMS Manager granska status för stängning, förnyelse eller korrigerande åtgärd och registrera resultatet i REG12.

10. Tillämpning av policyn

10.1 [All] När bristande efterlevnad av denna policy identifieras ska Privacy Lead / PIMS Manager registrera avvikelsen och den korrigerande åtgärden i REG12.

10.2 [Both] När obehörig AI-relaterad behandling, utlämnande eller åtkomst avseende PII, modellmissbruk, rättighetsbrist eller negativt integritetsutfall misstänks ska Incident Response Coordinator initiera incidenteskalering och registrera underlag i REG10 och REG12.

10.3 [Both] När ett personuppgiftsbiträde, underbiträde, en leverantör eller mottagare i ett upplägg för datadelning inte uppfyller AI-relaterade integritetsskyldigheter ska Vendor / Procurement Owner registrera åtgärdande, eskalering eller uppsägning i REG08 och REG12.

10.4 [All] När upprepade eller systemiska AI-relaterade integritetsavvikelser inträffar ska Top Management granska frågan och registrera ledningsåtgärden i REG12.

11. Granskning och underhåll

11.1 [All] Minst årligen ska Privacy Lead / PIMS Manager granska denna policy för fortsatt lämplighet och registrera granskningsresultatet i REG12.

11.2 [Conditional] När lagar, tjänster, modeller, datakällor, profileringspraxis, logik för automatiserat beslutsfattande, leverantörsarrangemang, överföringsrutter eller integritetsrisker ändras väsentligt ska Privacy Lead / PIMS Manager granska berörda AI-relaterade dataskyddskontroller och registrera resultatet i REG02, REG04 eller REG12.

11.3 [Controller] Minst årligen och efter väsentliga AI-relaterade ändringar av användarresan ska Process Owner / Business Owner granska underlag för transparens, meningsfull information, mänsklig granskning och rättighetsrutt samt registrera granskningen i REG06 och REG07.

11.4 [All] Efter att AI-relaterade korrigerande integritetsåtgärder har stängts ska Internal Audit / Compliance Reviewer verifiera effektiviteten och registrera verifieringsunderlag i REG12.

12. Relaterade policyer

12.1 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.3 PII03 - Policy för PII-behandlingsförteckning och rättslig grund

12.4 PII04 - Policy för integritetsmeddelande och transparens

12.5 PII05 - Policy för hantering av samtycke och preferenser

12.6 PII06 - Policy för hantering av registrerades rättigheter

12.7 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.8 PII08 - Policy för integritetsskydd genom design 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 avseende 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 PII-incidenter och hantering av personuppgiftsincidenter

12.16 PII17 - Policy för dokumenterad information och underlag i PIMS

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

12.18 PII19 - Policy för anställdas integritet

12.19 PII20 - Policy för barns integritet

12.20 PII22 - Policy för marknadsföringsintegritet och cookies

13. Referensstandarder och ramverk

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].