					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII06					Dokumenttitel: **Policy för hantering av registrerades rättigheter**							
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 7.5; Clause 8.1	Both	Primary	Underlag för rättighetsbegäranden och operativ styrning
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning, avvikelse och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Skyldigheter gentemot registrerade
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Invändning, tillgång, rättelse och radering
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Underrättelse till tredje part och kopia av behandlad PII
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Hantering av begäranden och skyldigheter vid automatiserat beslutsfattande
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Register över den personuppgiftsansvariges behandling
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Kundavtal, stöd för skyldigheter och personuppgiftsbiträdets register
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Personuppgiftsbiträdets stöd för skyldigheter gentemot registrerade
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Skydd av register över rättighetsbegäranden
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparens och ansvarsskyldighet
GDPR	Article 11; Article 12	Controller	Primary	Identifiering, former för begäranden, tidsfrister och styrning av svar
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Tillgång, rättelse och radering
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Begränsning, underrättelse och dataportabilitet

GDPR	Article 21; Article 22	Controller	Primary	Invändning och automatiserat beslutsfattande
GDPR	Article 24	Controller	Supporting	Den personuppgiftsansvariges ansvar och åtgärder
GDPR	Article 26	Joint Controller	Supporting	Ansvarsfördelning för rättigheter mellan gemensamt personuppgiftsansvariga
GDPR	Article 28	Both	Primary	Personuppgiftsbiträdets bistånd vid rättighetsbegäranden
GDPR	Article 30	Both	Supporting	Koppling till register över behandling
GDPR	Article 32	Both	Supporting	Säker hantering av underlag för rättigheter och utlämnanden
GDPR	Article 39	Conditional	Supporting	DPO-rådgivning och övervakning där det är tillämpligt
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparens, enskildas delaktighet, ansvarsskyldighet och efterlevnad
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Registrerades delaktighet och tillgång

1. Omfattning

1.1 Denna policy definierar obligatoriska krav för att ta emot, validera, bedöma, uppfylla, avslå, förlänga, stänga, övervaka och belägga rättighetsbegäranden från registrerade.

1.2 Denna policy gäller begäranden från registrerade eller behöriga företrädare avseende tillgång, rättelse, radering, begränsning, dataportabilitet, invändning, automatiserat beslutsfattande, vidarebefordran av återkallelse av samtycke, klagomål och relaterade förfrågningar.

1.3 Denna policy gäller i sammanhang där organisationen agerar som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde eller underbiträde.

1.4 Skyldigheter för personuppgiftsbiträden och underbiträden gäller endast när organisationen stöder en personuppgiftsansvarig, kund eller uppströms personuppgiftsbiträde enligt dokumenterade instruktioner.

1.5 Denna policy ersätter inte följande relaterade policyer:

1.5.1 PII03 för register över behandling och register över rättslig grund;

1.5.2 PII04 för innehåll i och publicering av integritetsmeddelanden;

1.5.3 PII05 för uppfyllande av samtycke och preferenser;

1.5.4 PII10 för genomförande av bevarande, radering och bortskaffning;

1.5.5 PII11 för styrning av korrekthet och kvalitet;

1.5.6 PII12 för livscykelstyrning av personuppgiftsbiträden och underbiträden;

1.5.7 PII15 för incident- och personuppgiftsincidenthantering.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att rättighetsbegäranden från registrerade hanteras konsekvent, lagenligt, säkert, inom definierade tidsramar och med revisionsklart underlag.

2.2 Denna policy säkerställer att organisationen kan visa ansvarsskyldighet för mottagande av begäranden, identitetsverifiering, bedömning, uppfyllande, avslag, förlängning, samarbete med personuppgiftsbiträden, stängning och ständig förbättring.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 Tillhandahålla konsekvent mottagning och uppföljning för alla rättighetsbegäranden från registrerade.

3.1.2 Verifiera den begärandes identitet eller behörighet före utlämnande, rättelse, radering, begränsning eller dataportabilitet.

3.1.3 Bedöma begäranden mot register över behandling, rollklassificering, rättsliga skyldigheter, avtalsförpliktelser och teknisk genomförbarhet.

3.1.4 Uppfylla giltiga begäranden inom dokumenterade tidsfrister.

3.1.5 Registrera underlag för avslag, delvis uppfyllande, förlängning och stängning.

3.1.6 Stödja den personuppgiftsansvariges skyldigheter när organisationen agerar som personuppgiftsbiträde eller underbiträde.

3.1.7 Skydda register över rättighetsbegäranden och svarspaket mot obehörigt röjande eller obehörig ändring.

3.1.8 Övervaka prestanda för rättighetsbegäranden och driva korrigerande åtgärder där så krävs.

4. Policyuttalanden

4.1 Mottagning, loggning och klassificering

4.1.1 [All] Privacy Lead / PIMS Manager ska registrera varje rättighetsbegäran från registrerade i REG06 inom två arbetsdagar från mottagandet.

4.1.2 [All] Privacy Lead / PIMS Manager ska klassificera varje typ av begäran, begärandekanal, datum för begäran, identitetsreferens för den begärande, utsedd ägare, intern förfallodag, lagstadgad eller avtalsenlig förfallodag samt aktuell status i REG06 innan bedömningen inleds.

4.1.3 [Controller] Privacy Lead / PIMS Manager ska bekräfta mottagandet eller lämna nästa erforderliga kommunikation till den begärande inom fem arbetsdagar från mottagandet och registrera kommunikationen i REG06.

4.1.4 [Controller] Process Owner / Business Owner ska koppla varje begäran till relevant behandlingsaktivitet i REG02 innan uppfyllandeåtgärder tilldelas.

4.1.5 [Joint Controller] Privacy Lead / PIMS Manager ska identifiera den part bland de gemensamt personuppgiftsansvariga som ansvarar för att hantera begäran i REG02, REG06 eller REG08 innan den sakliga bedömningen inleds.

4.1.6 [Processor] Privacy Lead / PIMS Manager ska registrera varje kundinstruktion som rör en rättighetsbegäran från registrerade i REG06 och REG08 innan stödaktiviteten inleds.

4.1.7 [Subprocessor] Vendor / Procurement Owner ska registrera varje uppströms instruktion som rör en rättighetsbegäran från registrerade i REG06 eller REG08 innan underbiträdets stödaktivitet inleds.

4.1.8 [All] Incident Response Coordinator ska registrera en eskalering i REG10 inom en arbetsdag när en rättighetsbegäran indikerar en möjlig PII-incident eller personuppgiftsincident.

4.2 Identitetsverifiering, omfattning och bedömning

4.2.1 [Controller] Privacy Lead / PIMS Manager ska verifiera den begärandes identitet eller företrädarens behörighet i REG06 innan PII lämnas ut eller en begärd ändring görs.

4.2.2 [Controller] Privacy Lead / PIMS Manager ska endast begära den minsta mängd ytterligare information som behövs för verifiering och registrera begäran i REG06 när identitet eller behörighet är otillräcklig.

4.2.3 [Controller] Process Owner / Business Owner ska identifiera relevanta system, poster, ändamål, PII-kategorier, mottagare och begränsningar kopplade till bevarande från REG02 innan uppfyllande bedöms.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor ska granska högriskbegäranden samt bestridda, oklara, överdrivna, upprepade, avslagna eller delvis uppfyllda begäranden i REG06 innan beslutet kommuniceras.

4.2.5 [Controller] System Owner / Application Owner ska verifiera att föreslagna svarsextrakt utesluter orelaterad PII och obehöriga tredjepartsuppgifter innan svarspaketet lämnas ut.

4.2.6 [Controller] Information Security Lead ska granska leveransmetoden för svar i REG06 eller REG12 innan stora mängder PII eller känslig PII, PII av särskilda kategorier eller PII med hög risk lämnas ut.

4.2.7 [Controller] Data Protection Officer / Privacy Advisor ska granska begäranden som rör automatiserat beslutsfattande eller profilering i REG06 och REG04 innan uppfyllande, avslag eller eskalering.

4.2.8 [Both] Privacy Lead / PIMS Manager ska registrera bedömningsresultat, tillämplig typ av begäran, beslut, motivering och nästa åtgärd i REG06 före uppfyllande eller avslag.

[... 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] Process Owner / Business Owner ska begära ett undantag i REG12 innan avvikelse sker från godkända krav för mottagning, verifiering, uppfyllande, svar eller stängning av rättighetsbegäranden.

9.1.2 [All] Privacy Lead / PIMS Manager ska godkänna eller avslå varje undantag för rättighetshantering i REG12 före införande.

9.1.3 [Controller] Data Protection Officer / Privacy Advisor ska granska varje undantag som rör avslag, delvis uppfyllande, osäker identitet, känslig PII, automatiserat beslutsfattande, begäranden som rör barn eller högriskbehandling före godkännande.

9.1.4 [Both] System Owner / Application Owner ska blockera utlämnande, rättelse, radering, begränsning eller export när ett erforderligt undantag inte har godkänts i REG12 före åtgärd.

9.1.5 [All] Privacy Lead / PIMS Manager ska tilldela utgångsdatum, ägare och kompenserande kontroll för varje godkänt undantag för rättighetshantering i REG12 innan undantaget blir aktivt.

10. Tillämpning

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera en avvikelse i REG12 inom fem arbetsdagar från identifiering av en försenad, saknad, ofullständig, overifierad eller ostödd post för rättighetsbegäran.

10.1.2 [Controller] System Owner / Application Owner ska stoppa utlämnande av svar tills kontroller av identitet, behörighet och svarspaket har registrerats i REG06.

10.1.3 [Both] Vendor / Procurement Owner ska eskalera bristande samarbete från personuppgiftsbiträde, underbiträde eller tredje part i REG08 och REG12 inom fem arbetsdagar från identifiering.

10.1.4 [All] Top Management ska tilldela ägarskap för korrigerande åtgärder i REG12 när brister i rättighetsbegäranden är systematiska, upprepade eller relevanta för certifiering.

10.1.5 [All] Internal Audit / Compliance Reviewer ska verifiera stängningsunderlag för rättighetsrelaterade korrigerande åtgärder i REG12 senast den tilldelade förfallodagen.

10.1.6 [All] Incident Response Coordinator ska initiera granskning i REG10 inom en arbetsdag när en avvikelse i en rättighetsbegäran indikerar obehörigt röjande, förlust, ändring, otillgänglighet eller annan misstänkt PII-incident.

11. Granskning och underhåll

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy årligen och registrera granskningsresultatet i REG12.

11.1.2 [All] Privacy Lead / PIMS Manager ska granska denna policy inom 30 dagar från väsentlig ändring av lagstiftning om rättighetsbegäranden, omfattning av behandlingsaktiviteter, verktyg för rättigheter, metod för identitetsverifiering, tjänstemodell för personuppgiftsbiträden eller PIMS-certifieringskrav.

11.1.3 [All] Data Protection Officer / Privacy Advisor ska granska integritetsmässigt betydande ändringar av denna policy 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 registrera kommunikation av godkända policyändringar i REG11 inom 30 dagar från publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

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 hantering av samtycke och preferenser

12.1.6 PII07 - Policy för integritetsriskbedömning och DPIA

12.1.7 PII08 - Policy för integritetsskydd genom design och som standard

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

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

12.1.10 PII11 - Policy för PII-korrekthet och kvalitet

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

12.1.12 PII13 - Policy för internationell överföring av PII

12.1.13 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.1.14 PII15 - Policy för PII-incidenter och personuppgiftsincidenter

12.1.15 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.1.16 PII17 - Policy för dokumenterad information och underlag inom PIMS

12.1.17 PII18 - Policy för övervakning, revision och förbättring inom PIMS

13. Referensstandarder och ramverk

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappat till dokumenterade register över rättighetsbegäranden, operativt arbetsflöde för begäranden, identitetsverifiering, uppfyllande, svar, stängning och underlag för stöd från personuppgiftsbiträden. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mappat till mätetal för rättighetsbegäranden, övervakning av försenade begäranden, revisionsstickprov, registrering av avvikelse, korrigerande åtgärder och verifiering av effektivitet. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Mappat till att fastställa och uppfylla skyldigheter gentemot registrerade genom dokumenterade rättighetskategorier, mottagningskanaler, verifiering, bedömning, svar och stängningskriterier. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mappat till hantering av invändning, tillgång, rättelse, radering och begränsning samt verifiering, uppfyllande och hantering av bestridd korrekthet. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mappat till underrättelse till tredje part efter rättighetsresultat och tillhandahållande av kopior eller portabla svarspaket. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mappat till dokumenterad hantering av legitima begäranden, tidsfrister, förlängningar, avslag, stängning och granskning av begäranden avseende automatiserat beslutsfattande. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Mappat till att koppla rättighetsbegäranden till register över behandling, behandlingsändamål, system, kategorier, mottagare och begränsningar kopplade till bevarande. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mappat till instruktioner i kundavtal, personuppgiftsbiträdets stöd för kundens skyldigheter och personuppgiftsbiträdets register över rättighetsstödjande aktiviteter. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Mappat till personuppgiftsbiträdets medel för att stödja den personuppgiftsansvariges skyldigheter gentemot registrerade, inklusive stöd för hämtning, rättelse, begränsning, radering och export enligt dokumenterad instruktion. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Mappat till skydd av register över rättighetsbegäranden, säker hantering av svarspaket, kontroller av svarsleverans och skydd av stängningsunderlag. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(2)** - Mappat till transparent rättighetshantering, underlag för ansvarsskyldighet, begärandeloggar, svarsregister, revisionsstickprov och korrigerande åtgärder. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Mappat till identifiering, ytterligare information när det är nödvändigt, svarstider, kommunikation, förlängning, avslag och stängning av begäran. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Mappat till sökresultat för tillgång, rättelse, radering, verifiering, underlag för uppfyllande och leverans av svarspaket. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Mappat till begränsning, underrättelse om rättighetsresultat till relevanta parter samt dataportabilitet eller leverans av kopia. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Mappat till bedömning av invändning och granskning av begäranden som rör automatiserat beslutsfattande eller profilering. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Mappat till den personuppgiftsansvariges styrningsåtgärder, roller, ägarskap för arbetsflöde, granskning, undantag, korrigerande åtgärder och ledningens tillsyn över rättighetshantering. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mappat till att identifiera ansvar för hantering av begäranden mellan gemensamt personuppgiftsansvariga innan den sakliga bedömningen inleds. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mappat till bistånd från personuppgiftsbiträden och underbiträden, dokumenterade kundinstruktioner, tidsfrister för stöd, inget direkt svar utan auktorisation och eskalering av bristande samarbete. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mappat till att koppla rättighetsbegäranden till register över behandling, behandlingsaktiviteter, system, PII-kategorier, mottagare och personuppgiftsbiträdens register. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mappat till säker hantering av rättighetsbegäranden, skydd av svarsleverans, förebyggande av obehörigt röjande och skydd av rättighetsunderlag. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mappat till rådgivning och övervakning från Data Protection Officer / Privacy Advisor för högriskbegäranden samt bestridda, avslagna, förlängda och automatiserat beslutsfattande-relaterade rättighetsbegäranden. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mappat till transparens för rättighetskanaler, enskildas delaktighet och tillgång, ansvarsskyldighet, klagomåls- och rättelseförfaranden, övervakning av integritetsefterlevnad och revisionsunderlag. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Mappat till registrerades delaktighet och tillgång, identitetsverifiering, tillgång, rättelse, radering, statusuppdateringar, stöd från personuppgiftsbiträden och mekanismer för klagomål och rättelse. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Interna krav

13.6.1 Internt krav - Klausuler som definierar REG06 som det primära rättighetsunderlaget, utbildning, godkännande av icke-standardiserat arbetsflöde, utgångsdatum för undantag, policygranskning och kommunikation av policyändringar stöder konsekvent genomförande men är inte direkt mappade till en enskild extern klausul. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].