					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII05					Dokumenttitel: **Policy för hantering av samtycke och preferenser**							
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	Dokumenterad information och operativ styrning för bevismaterial om samtycke
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning, avvikelse, korrigerande åtgärder och förbättring
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Supporting	Koppling till rättslig grund
ISO/IEC 27701:2025	Annex A.1.2.4; Annex A.1.2.5	Controller	Primary	Fastställande, inhämtning och registrering av samtycke
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Behandlingsregister för personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Avtal med personuppgiftsbiträde, kundändamål och biträdesregister
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Supporting	Personuppgiftsbiträdets stöd för den personuppgiftsansvariges skyldigheter gentemot registrerade
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Skydd av register över PII-behandling
GDPR	Article 4(11)	Controller	Supporting	Kriterier för samtycke
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Laglighet, korrekthet, öppenhet och ansvarsskyldighet
GDPR	Article 6(1)(a); Article 6(4)	Controller	Primary	Samtycke som rättslig grund och koppling vid ändrat ändamål
GDPR	Article 7	Controller	Primary	Villkor för samtycke och återkallelse
GDPR	Article 8	Conditional	Supporting	Eskalering av samtycke för barn
GDPR	Article 9(2)(a)	Conditional	Supporting	Uttryckligt samtycke för behandling av särskilda kategorier av uppgifter
GDPR	Article 24	Controller	Supporting	Personuppgiftsansvarigs ansvar och åtgärder

GDPR	Article 28	Both	Supporting	Koppling till biträdesinstruktioner och assistans
GDPR	Article 30	Both	Supporting	Koppling till register över behandlingsaktiviteter
ISO/IEC 29100:2020	Clause 5.2; Clause 5.8; Clause 5.12	Both	Supporting	Principer för samtycke och val, öppenhet och efterlevnad
ISO/IEC 29151:2022	Annex A.3	Both	Supporting	Kontroller för samtycke och val
ISO/IEC TS 27560:2023	Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4	Conditional	Supporting	Struktur för samtyckespost och samtyckeskvitto där sådana används

1. Omfattning

1.1 Denna policy fastställer obligatoriska krav för att avgöra när samtycke krävs, begära samtycke, samla in bevismaterial om samtycke, hantera preferenser, hantera återkallelser, upprätthålla samtyckesposter och granska samtyckesmekanismer.

1.2 Denna policy gäller för PII-behandling där samtycke väljs eller krävs som rättslig grund, där uttryckligt samtycke krävs, där samtyckespreferenser samlas in eller där organisationen hanterar samtyckesposter på uppdrag av en personuppgiftsansvarig.

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 samtyckesposter, preferensstatusar eller instruktioner om återkallelse hanteras enligt dokumenterade instruktioner från personuppgiftsansvarig eller kund.

1.5 Denna policy gör inte samtycke till den förvalda rättsliga grunden för PII-behandling.

1.6 Fastställande av rättslig grund regleras fortsatt av PII03 - Policy för PII-behandlingsregister och rättslig grund.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att hantering av samtycke och preferenser är laglig, transparent, möjlig att visa, återkallelig, tekniskt verkställbar och stöds av kontrollerat bevismaterial.

2.2 Denna policy säkerställer att samtycke endast begärs när det är lämpligt, att samtyckesposter är fullständiga och spårbara, att återkallelser respekteras samt att bevismaterial om samtycke finns tillgängligt för revision, förfrågningar och ansvarsskyldighet.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 Säkerställa att samtycke endast används när det är den lämpliga rättsliga grunden eller när det krävs för behandlingsaktiviteten.

3.1.2 Säkerställa att samtyckesbegäranden är specifika, informerade, urskiljbara och kopplade till tillämpligt integritetsmeddelande.

3.1.3 Säkerställa att samtyckes- och preferensposter samlas in och underhålls i REG05.

3.1.4 Säkerställa att återkallelser och preferensändringar hanteras inom fastställda operativa tidsramar.

3.1.5 Säkerställa att samtyckesposter kopplas till behandlingsändamål i REG02 och meddelandeversioner i REG07.

3.1.6 Säkerställa att aktiviteter där personuppgiftsbiträde och underbiträde stödjer samtycke följer dokumenterade instruktioner från personuppgiftsansvarig eller kund.

3.1.7 Säkerställa att samtyckesmekanismer övervakas, granskas, korrigeras och kan revideras.

4. Policyuttalanden

4.1 Tillämplighet för samtycke och rättslig grund

4.1.1 [Controller] Process Owner / Business Owner MUST registrera i REG02 om samtycke krävs eller har valts innan en ny eller väsentligt ändrad PII-behandlingsaktivitet som bygger på samtycke påbörjas.

4.1.2 [Controller] Privacy Lead / PIMS Manager MUST verifiera i REG02 och REG05 att samtycke inte har valts som förvald rättslig grund innan en ny eller väsentligt ändrad samtyckesbaserad behandlingsaktivitet godkänns.

4.1.3 [Controller] Data Protection Officer / Privacy Advisor MUST granska samtyckesgrunden i REG04 före lansering när behandlingen omfattar särskilda kategorier av PII, tjänster riktade till barn, högriskbehandling eller en obalans mellan organisationen och den registrerade.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager MUST dokumentera den part som ansvarar för att inhämta, registrera, förnya och respektera samtycke i REG02 och REG05 innan behandling med gemensamt personuppgiftsansvar påbörjas.

4.1.5 [Processor] Privacy Lead / PIMS Manager MUST registrera kundinstruktioner för insamling av samtycke, preferenshantering eller stöd vid återkallelse i REG08 och REG05 innan en samtyckesmekanism införs på uppdrag av en personuppgiftsansvarig.

4.1.6 [Subprocessor] Vendor / Procurement Owner MUST registrera samtyckesrelaterade skyldigheter för underbiträde i REG08 innan ett underbiträde får hantera samtyckesposter, preferensstatusar eller instruktioner om återkallelse.

4.2 Begäran och insamling av samtycke

4.2.1 [Controller] Process Owner / Business Owner MUST säkerställa att varje samtyckesbegäran är ändamålsspecifik och kopplad till tillämplig version av integritetsmeddelandet i REG07 innan samtyckesbegäran presenteras för en registrerad.

4.2.2 [Controller] System Owner / Application Owner MUST konfigurera samtyckesmekanismer så att de kräver en aktiv bekräftande åtgärd innan behandling påbörjas när uttryckligt samtycke eller opt-in-samtycke krävs.

4.2.3 [Controller] Process Owner / Business Owner MUST registrera referens till den registrerade, ändamål, PII-kategori, samtyckesformulering eller version, version av integritetsmeddelande, insamlingskanal, tidsstämpel, metod, status och tillämplig giltighetsperiod i REG05 när samtycke samlas in.

4.2.4 [Conditional] Privacy Lead / PIMS Manager MUST registrera logik för ålderssäkring eller behörighetskontroll i REG05 och initiera REG04-granskning före lansering när samtycket avser behandling riktad till barn.

4.2.5 [Conditional] Privacy Lead / PIMS Manager MUST markera samtycke som uttryckligt i REG05 innan behandling påbörjas när uttryckligt samtycke krävs för det valda ändamålet.

4.2.6 [Both] System Owner / Application Owner MUST förhindra att behandling som bygger på samtycke fortsätter innan REG05 visar aktiv samtyckesstatus för det relevanta ändamålet.

[... 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 MUST begära ett undantag i REG12 innan avvikelse sker från ett godkänt krav på insamling av samtycke, preferenshantering, återkallelse eller bevismaterial.

9.1.2 [All] Privacy Lead / PIMS Manager MUST godkänna eller avslå varje samtyckesrelaterat undantag i REG12 före införande och tilldela ett utgångsdatum och en kompenserande kontroll för varje godkänt undantag.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor MUST granska undantaget i REG04 eller REG12 före godkännande när undantaget omfattar uttryckligt samtycke, behandling riktad till barn, högriskbehandling eller en återkallelsemekanism.

9.1.4 [Both] System Owner / Application Owner MUST blockera produktionsrelease eller inaktivera den berörda samtyckesmekanismen när ett undantag som krävs enligt denna policy inte har godkänts i REG12 före produktionssättning.

10. Tillämpning

10.1.1 [All] Privacy Lead / PIMS Manager MUST registrera en samtyckesrelaterad avvikelse i REG12 inom fem arbetsdagar efter identifiering av saknat, ogiltigt, okopplat eller otillförlitligt bevismaterial om samtycke.

10.1.2 [Controller] Process Owner / Business Owner MUST avbryta eller åtgärda behandling för det berörda ändamålet innan ytterligare samtyckesbaserad behandling fortsätter när samtycke krävs men inte kan påvisas i REG05.

10.1.3 [Both] System Owner / Application Owner MUST inaktivera eller korrigera en avvikande samtyckes-, preferens- eller återkallelsemekanism inom den tidsram som tilldelats i REG12.

10.1.4 [Processor] Vendor / Procurement Owner MUST eskalera brister i kundinstruktioner som rör samtyckesposter, preferensstatusar eller stöd vid återkallelse i REG08 och REG12 inom fem arbetsdagar från identifiering.

10.1.5 [All] Internal Audit / Compliance Reviewer MUST verifiera stängningsbevis för samtyckesrelaterade korrigerande åtgärder i REG12 senast på tilldelat förfallodatum.

11. Granskning och underhåll

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

11.1.2 [All] Privacy Lead / PIMS Manager MUST granska denna policy inom 30 dagar från en väsentlig ändring av samtyckeslagstiftning, samtyckesteknik, verktyg för preferenshantering, struktur för integritetsmeddelanden eller krav för PIMS-certifiering.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUST granska integritetsväsentliga ändringar av denna policy i REG12 före godkännande.

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

11.1.5 [All] Privacy Lead / PIMS Manager MUST registrera kommunikation av godkända policyändringar i REG11 inom 30 dagar från publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII03 - Policy för PII-behandlingsregister och rättslig grund

12.5 PII04 - Policy för integritetsmeddelanden och öppenhet

12.6 PII06 - Policy för hantering av registrerades rättigheter

12.7 PII07 - Policy för integritetsriskbedömning och DPIA

12.8 PII08 - Policy för integritetsskydd genom design och 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 av PII

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

12.13 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.14 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.15 PII17 - Policy för dokumenterad information och bevismaterial inom PIMS

12.16 PII18 - Policy för PIMS-övervakning, revision och förbättring

13. Referensstandarder och ramverk

13.1 Denna policy är mappad mot följande standarder och regelverk. Mappningen förklarar hur policyn stöder de citerade kraven och identifierar de interna klausuler som genomför eller stöder dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mappas till dokumenterad information och operativ styrning för att fastställa samtyckets tillämplighet, samla in bevismaterial om samtycke, hantera återkallelse, versionshantera samtyckesposter, testa mekanismer och underhålla REG05. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.2; 4.5.3; 4.5.4; 7.1.1; 7.1.2; 7.1.3; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mappas till samtyckesövervakning, mätetal, revisionsstickprov, registrering av avvikelser, korrigerande åtgärder och verifiering av effektivitet. Addressed by clauses [4.5.5; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.2; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.2.3** - Mappas till att bekräfta när samtycke är en lämplig rättslig grund och att koppla samtyckesposter till REG02-poster om rättslig grund. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.2; 4.5.3].

13.2.4 **Annex A.1.2.4; Annex A.1.2.5** - Mappas till att fastställa när och hur samtycke inhämtas, samla in samtycke, registrera bevis, hantera uttryckligt samtycke, återkallelse, förnyelse och samtyckesstatus. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.5 **Annex A.1.2.9** - Mappas till personuppgiftsansvarigs register för samtyckesbaserad behandling, samtyckeshistorik, koppling till meddelanden, bevarande av bevismaterial och samtyckesposter med beredskap för revision. Addressed by clauses [4.2.3; 4.3.6; 4.5.1; 4.5.3; 7.1.1; 8.1.1; 8.1.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mappas till kundavtal för personuppgiftsbiträden, anpassning till kundens ändamål och instruktioner samt biträdesregister när samtyckesstödjande tjänster utförs för en personuppgiftsansvarig. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 8.1.4; 10.1.4].

13.2.7 **Annex A.2.3.2** - Mappas till personuppgiftsbiträdets stöd för den personuppgiftsansvariges skyldigheter gentemot registrerade när återkallelse av samtycke, preferensändringar eller bevismaterial om samtycke hanteras enligt kundinstruktion. Addressed by clauses [4.3.4; 4.3.5; 4.5.4; 6.1.4; 8.1.4].

13.2.8 **Annex A.3.14** - Mappas till skydd av samtyckes- och preferensposter mot obehörig ändring samt bevarande av bevismaterial för revisionsspår. Addressed by clauses [4.5.2; 5.1.6; 7.1.2; 10.1.5].

13.3 GDPR

13.3.1 **Article 4(11)** - Mappas till samtyckeskriterier som kräver att samtycke är specifikt, informerat, bekräftande där så krävs och kopplat till relevant ändamål och meddelandeversion. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.5].

13.3.2 **Article 5(1)(a); Article 5(2)** - Mappas till laglighet, korrekthet, öppenhet, bevismaterial för ansvarsskyldighet, revisionsstickprov, korrigerande åtgärder och bevis på samtyckesbaserad behandling. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.5.3; 4.5.5; 8.1.1; 8.1.5; 10.1.1; 10.1.5].

13.3.3 **Article 6(1)(a); Article 6(4)** - Mappas till samtycke som rättslig grund för specifika ändamål och till omprövning eller förnyat samtycke när ändamål eller behandlingsvillkor ändras väsentligt. Addressed by clauses [4.1.1; 4.1.2; 4.4.1; 4.4.2; 4.5.3].

13.3.4 Article 7 - Mappas till påvisbarhet, urskiljbara samtyckesbegäranden, återkallelse, enkel återkallelse, samtyckets giltighet och bevarad samtyckeshistorik. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.6; 4.4.4; 4.4.5; 10.1.2].

13.3.5 Article 8 - Mappas till eskalering av samtycke riktat till barn, logik för ålderssäkring eller behörighetskontroll samt granskning av integritetsrisk före lansering. Addressed by clauses [4.1.3; 4.2.4; 9.1.3].

13.3.6 **Article 9(2)(a)** - Mappas till hantering av uttryckligt samtycke när uttryckligt samtycke väljs för behandling av särskilda kategorier av uppgifter. Addressed by clauses [4.1.3; 4.2.5; 9.1.3].

13.3.7 **Article 24** - Mappas till styrningsåtgärder för personuppgiftsansvarig, granskning, godkännande, undantag, korrigerande åtgärder och ledningens tillsyn över samtyckeskontroller. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.2; 6.1.3; 9.1.1; 9.1.2; 11.1.1; 11.1.4].

13.3.8 **Article 28** - Mappas till hantering av instruktioner för personuppgiftsbiträde, bevismaterial för samtyckesstöd, stöd vid återkallelse, skyldigheter för underbiträden och eskalering av kundinstruktioner. Addressed by clauses [4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.5.4; 6.1.4; 7.1.4; 10.1.4].

13.3.9 **Article 30** - Mappas till koppling av samtyckesposter till behandlingsändamål, register för personuppgiftsansvarig, stödunderlag för personuppgiftsbiträde och spårbarhet mellan REG02 och REG05. Addressed by clauses [4.1.1; 4.5.3; 4.5.4; 7.1.1; 8.1.1].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.2; Clause 5.8; Clause 5.12** - Mappas till samtycke och val, öppenhet och koppling till meddelanden, återkallelse, ansvarsskyldighet och bevismaterial för efterlevnad av integritetskrav. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.5.3; 4.5.5; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3** - Mappas till kontroller för samtycke och val som kräver meningsfullt, informerat och otvetydigt samtycke, möjlighet att ändra preferenser samt skyndsamma behandlingsändringar efter ändring eller återkallelse av samtycke. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.4.5].

13.6 ISO/IEC TS 27560:2023

13.6.1 **Clause 5.2; Clause 6.2; Clause 6.3; Clause 6.4** - Mappas till begrepp för samtyckespost och samtyckeskvitto, registerföring av samtycke, struktur för samtyckespost, samtyckesstatus, koppling till meddelandeversion, kvittostruktur och tolkning av samtyckeskvitto när sådana poster eller kvitton används. Addressed by clauses [4.2.3; 4.3.2; 4.3.6; 4.4.3; 4.4.4; 4.5.2; 4.5.3; 7.1.6].

13.7 Interna krav

13.7.1 Internt krav - Klausuler som definierar REG05 som auktoritativt bevisobjekt, godkännande av icke-standardiserat bevismaterial, blockering av operativ release, utbildning, policyunderhåll och kommunikation stöder konsekvent genomförande men är inte direkt mappade till en enskild extern klausul. Addressed by clauses [4.5.1; 5.1.2; 7.1.5; 9.1.4; 11.1.2; 11.1.3; 11.1.5].