| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ange namnet på den registrerade juridiska personen här | | | | | | | |
| Dokumentnummer:<br>PII02 | | | | | Dokumenttitel:<br>**Policy för roller, ansvar och ansvarsskyldighet inom integritetsskydd** | | | | | | | |
| Version:<br>1.0 | | Ikraftträdandedatum:<br>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 4.1 | Both | Primary | Kontext för PIMS-roll |
| ISO/IEC 27701:2025 | Clause 5.1 | Both | Primary | Ledarskap och ansvarsskyldighet |
| ISO/IEC 27701:2025 | Clause 5.3 | Both | Primary | PIMS-roller, ansvar och befogenheter |
| ISO/IEC 27701:2025 | Clause 7.2 | Both | Primary | Rollkompetens |
| ISO/IEC 27701:2025 | Clause 7.3 | Both | Primary | Rollmedvetenhet |
| ISO/IEC 27701:2025 | Clause 7.4 | Both | Supporting | Rollkommunikation |
| ISO/IEC 27701:2025 | Clause 7.5 | Both | Primary | Dokumenterad information om roller |
| ISO/IEC 27701:2025 | Clause 8.1 | Both | Primary | Ägarskap för operativ styrning |
| ISO/IEC 27701:2025 | Clause 9.2 | Both | Supporting | Oberoende revisionsroll |
| ISO/IEC 27701:2025 | Clause 9.3 | Both | Supporting | Ledningens genomgång av ansvarsskyldighet |
| ISO/IEC 27701:2025 | Clause 10.2 | Both | Supporting | Rollrelaterad avvikelse och korrigerande åtgärder |
| ISO/IEC 27701:2025 | Annex A.1.2.7 | Controller | Supporting | Ansvar för biträdesavtal |
| ISO/IEC 27701:2025 | Annex A.1.2.8 | Joint Controller | Primary | Roller och ansvar för gemensamt personuppgiftsansvarig |
| ISO/IEC 27701:2025 | Annex A.1.2.9 | Controller | Primary | Underlag för ansvarsskyldighet |
| ISO/IEC 27701:2025 | Annex A.2.2.2 | Processor | Primary | Kundavtal och instruktioner för personuppgiftsbiträde |
| ISO/IEC 27701:2025 | Annex A.2.2.3 | Processor | Supporting | Ändamålsanpassning för personuppgiftsbiträde |
| GDPR | Article 5(2) | Controller | Supporting | Underlag för ansvarsskyldighet |
| GDPR | Article 24 | Controller | Supporting | Personuppgiftsansvarigs ansvar och åtgärder |

| | | | | |
|---|---|---|---|---|
| GDPR | Article 26 | Joint Controller | Supporting | Arrangemang för gemensamt personuppgiftsansvarig |
| GDPR | Article 28 | Both | Supporting | Styrning av personuppgiftsbiträde och instruktioner |
| GDPR | Article 30 | Both | Supporting | Behandlingsregister och underlag för ansvar |
| GDPR | Article 37 | Conditional | Referenced | Utnämning av DPO när tillämpligt |
| GDPR | Article 38 | Conditional | Supporting | DPO:s ställning och oberoende när tillämpligt |
| GDPR | Article 39 | Conditional | Supporting | DPO:s uppgifter när tillämpligt |
| ISO/IEC 29100:2020 | Clause 4.1; Clause 4.2 | Both | Supporting | Aktörer och roller i ramverk för integritetsskydd |
| ISO/IEC 29100:2020 | Clause 5.12 | Both | Supporting | Ansvarsskyldighet för efterlevnad inom integritetsskydd |
| ISO/IEC 29151:2022 | Clause 6.1.2; Clause 6.1.3 | Both | Supporting | Roller och funktionsuppdelning för skydd av PII |
| ISO/IEC 27002:2022 | Control 5.2 | Both | Supporting | Roller och ansvar för informationssäkerhet |
| ISO/IEC 27002:2022 | Control 5.3 | Both | Supporting | Funktionsuppdelning |

## 1. Omfattning

1.1 Denna policy definierar PIMS-rollmodellen, ansvarsskyldighetsstrukturen, regler för ansvarstilldelning, regler för rollkombination, förväntningar på eskalering och krav på underlag för integritetsstyrning.

1.2 Denna policy gäller för personal, funktioner, system, leverantörer, personuppgiftsbiträden, underbiträden och relationer med gemensamt personuppgiftsansvarig som deltar i eller påverkar behandling av PII inom PIMS-omfattningen.

1.3 Denna policy gäller i sammanhang som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde.

1.4 Denna policy skapar inte nya organisatoriska befattningsbenämningar.

1.5 Denna policy definierar kanoniska PIMS-roller som kan tilldelas befintlig personal eller befintliga funktioner, förutsatt att rolltilldelning, kompetens, oberoende och krav avseende intressekonflikt dokumenteras.

## 2. Syfte

2.1 Syftet med denna policy är att säkerställa att PIMS-ansvar är tydligt tilldelat, förstått, kommunicerat, styrkt med underlag, granskat och förbättrat.

2.2 Denna policy gör det möjligt för organisationen att visa ansvarsskyldighet för integritetsstyrning, ägarskap för behandling av PII, fastställande av roller som personuppgiftsansvarig och personuppgiftsbiträde, ansvarsfördelning vid gemensamt personuppgiftsansvar, hantering av instruktioner till personuppgiftsbiträde, leverantörers integritetsansvar, oberoende granskning och rollbaserad eskalering.

## 3. Mål

### 3.1 Målen med denna policy är att:

3.1.1 definiera de kanoniska PIMS-roller som används i hela PIMS-policyuppsättningen;

3.1.2 säkerställa att varje väsentligt PIMS-ansvar har en tilldelad ansvarig roll;

3.1.3 stödja ansvarsskyldighet för personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde;

3.1.4 tillåta praktisk rollkombination för små och medelstora organisationer samtidigt som intressekonflikter kontrolleras;

3.1.5 bevara oberoende granskning genom Internal Audit / Compliance Reviewer;

3.1.6 säkerställa att rolltilldelningar och rolländringar registreras i kanoniska evidensobjekt;

3.1.7 säkerställa att innehavare av PIMS-roller får lämplig kommunikation och medvetenhet;

3.1.8 säkerställa att rollrelaterade luckor, konflikter och avvikelser eskaleras och korrigeras.

## 4. Policyuttalanden

### 4.1 PIMS-rollmodell och tilldelning

4.1.1 [All] Top Management ska godkänna den kanoniska PIMS-rollmodellen i REG01 före det initiala införandet av PIMS och därefter årligen.

4.1.2 [All] Privacy Lead / PIMS Manager ska underhålla namngivna PIMS-rolltilldelningar i REG01 före införandet av PIMS och inom 10 arbetsdagar efter personal- eller organisationsförändringar.

4.1.3 [All] Privacy Lead / PIMS Manager ska dokumentera ansvarsomfattning och befogenhetsnivå för varje tilldelad PIMS-roll i REG01 innan tilldelningen träder i kraft.

4.1.4 [All] Process Owner / Business Owner ska tilldela en ansvarig behandlingsägare för varje behandlingsaktivitet av PII i REG02 innan behandlingsaktiviteten inleds.

4.1.5 [All] System Owner / Application Owner ska dokumentera ansvarig systemägare för varje system som behandlar PII i REG02 innan systemet tas i produktion.

4.1.6 [All] Vendor / Procurement Owner ska dokumentera relationsägaren för varje relation med personuppgiftsbiträde, underbiträde, tredjepartsdelning av data eller gemensamt personuppgiftsansvarig i REG08 före introduktion eller godkännande av avtal.

### 4.2 Rollkombination, funktionsuppdelning och oberoende

4.2.1 [All] Privacy Lead / PIMS Manager ska dokumentera varje PIMS-rollkombination i REG01 innan rollkombinationen träder i kraft.

4.2.2 [All] Top Management ska godkänna rollkombinationer som omfattar Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator eller Internal Audit / Compliance Reviewer i REG01 före tilldelning.

4.2.3 [All] Internal Audit / Compliance Reviewer ska dokumentera sitt oberoende från den PIMS-process som granskas i REG12 innan varje PIMS-revision eller efterlevnadsgranskning inleds.

4.2.4 [All] Privacy Lead / PIMS Manager ska registrera kompenserande kontroller för oundvikliga konflikter i funktionsuppdelningen i REG12 innan en rollkombination godkänns.

4.2.5 [All] Data Protection Officer / Privacy Advisor ska registrera farhågor om rolloberoende eller intressekonflikt i REG12 inom fem arbetsdagar efter identifiering.

[ ... 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 från rollbaserad ansvarsskyldighet i REG12 innan en behandlingsaktivitet av PII bedrivs utan en obligatorisk tilldelad roll.

9.1.2 [All] Privacy Lead / PIMS Manager ska bedöma konsekvensen och riskbegränsningen för varje undantag från rollbaserad ansvarsskyldighet i REG12 inom 10 arbetsdagar efter begäran.

9.1.3 [All] Top Management ska godkänna undantag från rollbaserad ansvarsskyldighet som överstiger 30 dagar eller påverkar högriskbehandling i REG12 innan undantaget träder i kraft.

9.1.4 [All] Privacy Lead / PIMS Manager ska ange ett utgångsdatum som inte överstiger 90 dagar i REG12 för varje godkänt undantag från rollbaserad ansvarsskyldighet före godkännande.

9.1.5 [All] Privacy Lead / PIMS Manager ska stänga eller ompröva varje undantag från rollbaserad ansvarsskyldighet i REG12 inom fem arbetsdagar efter utgångsdatumet.

## 10. Tillämpning

10.1.1 [All] Privacy Lead / PIMS Manager ska registrera saknade, felaktiga eller inaktuella PIMS-rolltilldelningar som avvikelser i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [All] Top Management ska kräva korrigerande åtgärder i REG12 inom 15 arbetsdagar vid upprepade eller långvariga brister i ansvarsskyldighet.

10.1.3 [All] Process Owner / Business Owner ska förhindra att ny eller ändrad behandling av PII tas i produktion när obligatoriskt roll- och ansvarsskyldighetsunderlag saknas i REG02 eller REG08.

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

## 11. Granskning och underhåll

11.1.1 [All] Privacy Lead / PIMS Manager ska granska denna policy årligen och inom 30 dagar efter väsentlig ändring av PIMS-rollmodellen.

11.1.2 [All] Data Protection Officer / Privacy Advisor ska granska föreslagna ändringar av denna policy med avseende på påverkan på integritetsroller i REG12 före godkännande.

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

11.1.4 [All] Privacy Lead / PIMS Manager ska uppdatera REG01 och REG11 inom 15 arbetsdagar efter godkända ändringar av PIMS-roller, ansvar eller kommunikationskrav.

## 12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII03 - Policy för register över PII-behandling och rättslig grund

12.4 PII07 - Policy för integritetsriskbedömning och DPIA

12.5 PII08 - Policy för inbyggt dataskydd och dataskydd som standard

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

12.7 PII14 - Policy för PII-säkerhet och åtkomstkontroll

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

12.9 PII16 - Policy för integritetsutbildning, medvetenhet och kompetens

12.10 PII17 - Policy för dokumenterad information och evidenshantering inom PIMS

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

## 13. Referensstandarder och ramverk

13.1 Denna policy är mappad till 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 4.1** - Mappad till fastställande av PIMS-rollkontext, tillämplighet för personuppgiftsansvarig och personuppgiftsbiträde, behandlingsägarskap och register över relationsansvar. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mappad till godkännande av Top Management, tillsyn över ansvarsskyldighet, årlig ledningsgenomgång, mätetal för ansvarsskyldighet och korrigerande åtgärder vid rollbrister. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mappad till tilldelning, dokumentation, kommunikation och underhåll av PIMS-roller, ansvar, befogenheter, systemägarskap, behandlingsägarskap, ägarskap för leverantörsrelationer, ägarskap för incidenteskalering och ansvar för oberoende granskning. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mappad till rollspecifik kompetens och medvetenhetsunderlag för tilldelade PIMS-ansvar. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mappad till medvetenhet om tilldelade PIMS-ansvar, underlag för bekräftelse och årlig rapportering av rollmedvetenhet. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mappad till kommunikation av rolltilldelningar, rolländringar, eskaleringar och information om rollöverlämning. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mappad till dokumenterad information för PIMS-rolltilldelningar, ansvarsomfattningar, befogenhetsnivåer, årligt bevarande av underlag och underhåll av rollmatris. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mappad till ägarskap för operativ styrning av behandlingsaktiviteter, system, leverantörer, personuppgiftsbiträden, underbiträden, relationer med gemensamt personuppgiftsansvarig och kontroller före produktionssättning. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mappad till oberoende revision och efterlevnadsgranskning av underlag för rolltilldelning, underlag för rollkombination, underlag för oberoende, iakttagelser och stängning av korrigerande åtgärder. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mappad till ledningens genomgång av fullständighet i PIMS-rolltilldelning, rollkonflikter, undantag, mätetal för ansvarsskyldighet och resultat från granskning av ansvarsskyldighet. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mappad till eskalering, registrering av avvikelser, korrigerande åtgärder, stängning av undantag och verifiering av effektivitet för frågor om rollbaserad ansvarsskyldighet. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mappad till tilldelning och dokumentation av ansvar för biträdesavtal samt eskalering av tredjepartsansvar före godkännande eller förnyelse av avtal. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mappad till dokumentation av ansvarsfördelning för gemensamt personuppgiftsansvarig och underlag för relationsansvar innan behandling inom gemensamt personuppgiftsansvar inleds. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mappad till underhåll av register över ansvarsskyldighet för behandlingsägarskap hos personuppgiftsansvarig, rollklassificering och evidensägarskap. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mappad till ansvar för kundavtal för personuppgiftsbiträde, ägarskap för kundinstruktioner och underlag för biträdesrelationer. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mappad till anpassning av personuppgiftsbiträdets ändamål och instruktioner genom ägarskap för kundinstruktioner och verifiering av roller som personuppgiftsansvarig/personuppgiftsbiträde. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

**13.3 GDPR**

13.3.1 **Article 5(2)** - Mappad till underlag för ansvarsskyldighet avseende rolltilldelningar, behandlingsägarskap, rollgranskningar, avvikelser och revisionsiakttagelser. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mappad till personuppgiftsansvarigs ansvar, ansvarigt behandlingsägarskap, tillsyn av Top Management, årlig granskning och åtgärder för ansvarsskyldighet. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mappad till dokumentation av ansvarsfördelning för gemensamt personuppgiftsansvarig och underlag för relationsansvar innan behandling inom gemensamt personuppgiftsansvar inleds. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mappad till ansvarsfördelning för personuppgiftsbiträde och underbiträde, ägarskap för kundinstruktioner, avtalsansvar och eskaleringsvägar för tredje part. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mappad till behandlingsregister, behandlingsägarskap, PIMS-rollklassificering och verifiering av roller som personuppgiftsansvarig/personuppgiftsbiträde. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mappad till dokumentation av rollen Data Protection Officer / Privacy Advisor när utnämning är tillämplig eller frivilligt tilldelad. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mappad till ställning, oberoende, delaktighet och hantering av intressekonflikter för Data Protection Officer / Privacy Advisor där tillämpligt. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mappad till integritetsrådgivning, övervakningsobservationer, rådgivande granskning och rollrelaterad granskning av integritetspåverkan av Data Protection Officer / Privacy Advisor där tillämpligt. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

**13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 4.1; Clause 4.2** - Mappad till aktörer i ramverk för integritetsskydd och rollfördelning för PII-principaler, personuppgiftsansvariga för PII, personuppgiftsbiträden för PII, tredje parter och PIMS-rollklassificering. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mappad till ansvarsskyldighet för integritetsefterlevnad, rollunderlag, granskning, revisionsiakttagelser och verifiering av korrigerande åtgärder. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

**13.5 ISO/IEC 29151:2022**

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mappad till definition av roller för PII-skydd, rolldokumentation, rollkommunikation, samordning mellan säkerhet och integritet samt funktionsuppdelning för PII-skydd. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

**13.6 ISO/IEC 27002:2022**

13.6.1 Control 5.2 - Mappad till definition, fördelning, dokumentation, kommunikation och underhåll av PIMS-ansvar och informationssäkerhetsansvar. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mappad till funktionsuppdelning, godkännande av rollkombination, oberoende granskning, konfliktkontroller och verifiering av korrigerande åtgärder för rollkonflikter. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].