					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII02					Dokumenttitel: **Politik for databeskyttelsesroller, ansvarsområder og ansvarlighed**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	PIMS-rollekontekst
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Ledelse og ansvarlighed
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS-roller, ansvar og beføjelser
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Rollekompetence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Rollebevidsthed
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Rollekommunikation
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenteret information om roller
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Ejerskab til operationel styring
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Uafhængig revisionsrolle
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Ledelsens gennemgang af ansvarlighed
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Rollerelateret afvigelse og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Ansvar for databehandlerkontrakt
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Fælles dataansvarliges roller og ansvar
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Ansvarlighedsregistreringer
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Databehandlers kundeaftaler og instrukser
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Databehandlers formålsmæssige tilpasning
GDPR	Article 5(2)	Controller	Supporting	Bevismateriale for ansvarlighed
GDPR	Article 24	Controller	Supporting	Dataansvarliges ansvar og foranstaltninger
GDPR	Article 26	Joint Controller	Supporting	Ordninger mellem fælles dataansvarlige

GDPR	Article 28	Both	Supporting	Styring af databehandler og instrukser
GDPR	Article 30	Both	Supporting	Behandlingsfortegnelser og bevismateriale for ansvar
GDPR	Article 37	Conditional	Referenced	Udpegning af DPO, hvor det er relevant
GDPR	Article 38	Conditional	Supporting	DPO's stilling og uafhængighed, hvor det er relevant
GDPR	Article 39	Conditional	Supporting	DPO's opgaver, hvor det er relevant
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Aktører og roller i privatlivsrammen
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Ansvarlighed for efterlevelse af databeskyttelse
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Roller og funktionsadskillelse for beskyttelse af PII
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Informationssikkerhedsroller og ansvar
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Funktionsadskillelse

1. Omfang

1.1 Denne politik fastlægger PIMS-rollemodellen, ansvarlighedsstrukturen, regler for tildeling af ansvar, regler for rollekombination, forventninger til eskalering og krav til bevismateriale for styring af databeskyttelse.

1.2 Denne politik gælder for personale, funktioner, systemer, leverandører, databehandlere, underdatabehandlere og relationer mellem fælles dataansvarlige, som deltager i eller påvirker behandling af PII inden for PIMS-omfang.

1.3 Denne politik gælder på tværs af kontekster som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler.

1.4 Denne politik opretter ikke nye organisatoriske stillingsbetegnelser. Den definerer kanoniske PIMS-roller, som kan tildeles eksisterende personale eller funktioner, forudsat at rolletildeling, kompetence, uafhængighed og krav vedrørende interessekonflikt dokumenteres.

2. Formål

2.1 Formålet med denne politik er at sikre, at PIMS-ansvar er klart tildelt, forstået, kommunikeret, dokumenteret med bevismateriale, gennemgået og forbedret.

2.2 Denne politik gør organisationen i stand til at dokumentere ansvarlighed for styring af databeskyttelse, ejerskab til PII-behandling, fastlæggelse af roller som dataansvarlig og databehandler, fordeling af ansvar mellem fælles dataansvarlige, håndtering af instrukser til databehandler, leverandørers ansvar for databeskyttelse, uafhængig gennemgang og rollebaseret eskalering.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 definere de kanoniske PIMS-roller, der anvendes på tværs af PIMS-politiksættet;

3.1.2 sikre, at ethvert væsentligt PIMS-ansvar har en tildelt ansvarlig rolle;

3.1.3 understøtte ansvarlighed som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler;

3.1.4 tillade praktisk rollekombination for små og mellemstore organisationer, samtidig med at interessekonflikter kontrolleres;

3.1.5 bevare uafhængig gennemgang ved Internal Audit / Compliance Reviewer;

3.1.6 sikre, at rolletildelinger og rolleændringer registreres i kanoniske evidensobjekter;

3.1.7 sikre, at PIMS-rolleindehavere modtager relevant kommunikation og bevidstgørelse;

3.1.8 sikre, at rollerelaterede mangler, konflikter og afvigelser eskaleres og korrigeres.

4. Politikkerklæringer

4.1 PIMS-rollemodel og tildeling

4.1.1 [All] Top Management skal godkende den kanoniske PIMS-rollemodel i REG01 før den første PIMS-implementering og derefter årligt.

4.1.2 [All] Privacy Lead / PIMS Manager skal vedligeholde navngivne PIMS-rolletildelinger i REG01 før PIMS-implementering og senest 10 arbejdsdage efter personale- eller organisationsændringer.

4.1.3 [All] Privacy Lead / PIMS Manager skal dokumentere ansvarsområde og beføjelsesniveau for hver tildelt PIMS-rolle i REG01, før tildelingen træder i kraft.

4.1.4 [All] Process Owner / Business Owner skal tildele en ansvarlig behandlingsejer for hver PII-behandlingsaktivitet i REG02, før behandlingsaktiviteten påbegyndes.

4.1.5 [All] System Owner / Application Owner skal dokumentere den ansvarlige systemejer for hvert system, der behandler PII, i REG02 før idriftsættelse i produktionsmiljøet.

4.1.6 [All] Vendor / Procurement Owner skal dokumentere relationsejeren for hver databehandler, underdatabehandler, tredjepartsdeling af data eller relation mellem fælles dataansvarlige i REG08 før onboarding eller godkendelse af aftale.

4.2 Rollekombination, funktionsadskillelse og uafhængighed

4.2.1 [All] Privacy Lead / PIMS Manager skal dokumentere hver PIMS-rollekombination i REG01, før rollekombinationen træder i kraft.

4.2.2 [All] Top Management skal godkende rollekombinationer, der involverer Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator eller Internal Audit / Compliance Reviewer, i REG01 før tildeling.

4.2.3 [All] Internal Audit / Compliance Reviewer skal dokumentere uafhængighed af den PIMS-proces, der gennemgås, i REG12 før hver PIMS-revision eller efterlevelsesgennemgang påbegyndes.

4.2.4 [All] Privacy Lead / PIMS Manager skal registrere kompenserende kontroller for uundgåelige konflikter vedrørende funktionsadskillelse i REG12, før en rollekombination godkendes.

4.2.5 [All] Data Protection Officer / Privacy Advisor skal registrere bekymringer om rolleuafhængighed eller interessekonflikt i REG12 senest fem arbejdsdage efter identifikation.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Undtagelser

9.1.1 [All] Process Owner / Business Owner skal anmode om en undtagelse vedrørende rolleansvarlighed i REG12, før en PII-behandlingsaktivitet drives uden en krævet tildelt rolle.

9.1.2 [All] Privacy Lead / PIMS Manager skal vurdere konsekvens og afbødning for hver undtagelse vedrørende rolleansvarlighed i REG12 senest 10 arbejdsdage efter anmodning.

9.1.3 [All] Top Management skal godkende undtagelser vedrørende rolleansvarlighed, der overstiger 30 dage eller påvirker højrisikobehandling, i REG12, før undtagelsen træder i kraft.

9.1.4 [All] Privacy Lead / PIMS Manager skal fastsætte en udløbsdato på højst 90 dage i REG12 for hver godkendt undtagelse vedrørende rolleansvarlighed før godkendelse.

9.1.5 [All] Privacy Lead / PIMS Manager skal lukke eller revurdere hver undtagelse vedrørende rolleansvarlighed i REG12 senest fem arbejdsdage efter udløb.

10. Håndhævelse

10.1.1 [All] Privacy Lead / PIMS Manager skal registrere manglende, unøjagtige eller forældede PIMS-rolletildelinger som afvigelser i REG12 senest fem arbejdsdage efter identifikation.

10.1.2 [All] Top Management skal kræve korrigerende handling i REG12 senest 15 arbejdsdage efter gentagne eller langvarige ansvarlighedssvigt.

10.1.3 [All] Process Owner / Business Owner skal forhindre idriftsættelse i produktionsmiljøet af ny eller ændret PII-behandling, hvor krævet bevismateriale for rolle og ansvarlighed mangler i REG02 eller REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer skal verificere effektiviteten af korrigerende handlinger for afvigelser vedrørende rolleansvarlighed i REG12 ved næste planlagte revision eller senest 60 dage efter lukning, alt efter hvad der indtræffer først.

11. Gennemgang og vedligeholdelse

11.1.1 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik årligt og senest 30 dage efter en væsentlig ændring af PIMS-rollemodellen.

11.1.2 [All] Data Protection Officer / Privacy Advisor skal gennemgå foreslåede ændringer af denne politik med henblik på påvirkning af databeskyttelsesroller i REG12 før godkendelse.

11.1.3 [All] Top Management skal godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.

11.1.4 [All] Privacy Lead / PIMS Manager skal opdatere REG01 og REG11 senest 15 arbejdsdage efter godkendte ændringer af PIMS-roller, ansvar eller kommunikationskrav.

12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII01 - Politik for ledelsessystem for privatlivsinformation

12.3 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag

12.4 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.5 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.6 PII12 - Politik for styring af databehandlere, underdatabehandlere og tredjeparters databeskyttelse

12.7 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.8 PII15 - Politik for PII-hændelser og håndtering af brud

12.9 PII16 - Politik for træning, bevidstgørelse og kompetence vedrørende databeskyttelse

12.10 PII17 - Politik for dokumenteret information og styring af bevismateriale i PIMS

12.11 PII18 - Politik for overvågning, revision og forbedring af PIMS

13. Referencestandarder og rammeværker

13.1 Denne politik er kortlagt til følgende standarder og regler. Kortlægningen forklarer, hvordan politikken understøtter de citerede krav og identificerer de interne klausuler, der implementerer eller understøtter dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Kortlagt til fastlæggelse af PIMS-rollekontekst, anvendelighed som dataansvarlig og databehandler, behandlingsejerskab og registreringer af relationsansvar. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Kortlagt til godkendelse fra Top Management, tilsyn med ansvarlighed, årlig ledelsesgennemgang, ansvarlighedsmetrikker og korrigerende handling ved rollesvigt. 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** - Kortlagt til tildeling, dokumentation, kommunikation og vedligeholdelse af PIMS-roller, ansvar, beføjelser, systemejerskab, behandlingsejerskab, ejerskab til leverandørrelationer, ejerskab til hændelseseskalering og ansvar for uafhængig gennemgang. 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** - Kortlagt til rollespecifik kompetence og bevismateriale for bevidstgørelse vedrørende tildelte PIMS-ansvarsområder. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Kortlagt til bevidsthed om tildelte PIMS-ansvarsområder, bevismateriale for bekræftelse og årlig rapportering om rollebevidsthed. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Kortlagt til kommunikation af rolletildelinger, rolleændringer, eskaleringer og information om rolleoverdragelse. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Kortlagt til dokumenteret information om PIMS-rolletildelinger, ansvarsområder, beføjelsesniveauer, årlig opbevaring af bevismateriale og vedligeholdelse af rollematrice. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Kortlagt til ejerskab til operationel styring for behandlingsaktiviteter, systemer, leverandører, databehandlere, underdatabehandlere, relationer mellem fælles dataansvarlige og kontroller ved idriftsættelse i produktionsmiljøet. 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** - Kortlagt til uafhængig revision og efterlevelsesgennemgang af bevismateriale for rolletildeling, bevismateriale for rollekombination, bevismateriale for uafhængighed, konstateringer og lukning af korrigerende handlinger. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Kortlagt til ledelsens gennemgang af fuldstændighed i PIMS-rolletildelinger, rollekonflikter, undtagelser, ansvarlighedsmetrikker og resultater af ansvarlighedsgennemgang. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Kortlagt til eskalering, registrering af afvigelser, korrigerende handling, lukning af undtagelser og verifikation af effektivitet for forhold vedrørende rolleansvarlighed. 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** - Kortlagt til tildeling og dokumentation af ansvar for databehandlerkontrakter og eskalering af tredjepartsansvar før kontraktgodkendelse eller fornyelse. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Kortlagt til dokumentation af ansvarsfordeling mellem fælles dataansvarlige og bevismateriale for relationsansvar, før behandling som fælles dataansvarlige påbegyndes. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Kortlagt til vedligeholdelse af ansvarlighedsregistreringer for ejerskab til behandling som dataansvarlig, rolleklassifikation og ejerskab til bevismateriale. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Kortlagt til ansvar for databehandlers kundeaftaler, ejerskab til kundeinstrukser og bevismateriale for databehandlerrelationer. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Kortlagt til tilpasning af databehandlers formål og instrukser gennem ejerskab til kundeinstrukser og verifikation af roller som dataansvarlig/databehandler. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Kortlagt til bevismateriale for ansvarlighed vedrørende rolletildelinger, behandlingsejerskab, rollegennemgange, afvigelser og revisionskonstateringer. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Kortlagt til dataansvarliges ansvar, ansvarligt behandlingsejerskab, tilsyn fra Top Management, årlig gennemgang og ansvarlighedsforanstaltninger. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Kortlagt til dokumentation af ansvarsfordeling mellem fælles dataansvarlige og bevismateriale for relationsansvar, før behandling som fælles dataansvarlige påbegyndes. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Kortlagt til ansvarsfordeling for databehandler og underdatabehandler, ejerskab til kundeinstrukser, kontraktansvar og eskalationsveje for tredjeparter. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Kortlagt til behandlingsfortegnelser, behandlingsejerskab, PIMS-rolleklassifikation og verifikation af roller som dataansvarlig/databehandler. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Kortlagt til dokumentation af rollen Data Protection Officer / Privacy Advisor, hvor udpegning er relevant eller frivilligt tildelt. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Kortlagt til stilling, uafhængighed, inddragelse og håndtering af interessekonflikter for Data Protection Officer / Privacy Advisor, hvor det er relevant. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Kortlagt til rådgivning om databeskyttelse, overvågningsobservationer, rådgivende gennemgang og rollerelateret gennemgang af påvirkning på databeskyttelse ved Data Protection Officer / Privacy Advisor, hvor det er relevant. 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** - Kortlagt til aktører i privatlivsrammen og rollefordeling for registrerede, PII dataansvarlige, PII databehandlere, tredjeparter og PIMS-rolleklassifikation. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Kortlagt til ansvarlighed for efterlevelse af databeskyttelse, rollebevismateriale, gennemgang, revisionskonstateringer og verifikation af korrigerende handlinger. 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** - Kortlagt til definition af roller for PII-beskyttelse, rolledokumentation, rollekommunikation, koordinering mellem sikkerhed og databeskyttelse samt funktionsadskillelse for PII-beskyttelse. 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 - Kortlagt til definition, tildeling, dokumentation, kommunikation og vedligeholdelse af PIMS-ansvar og informationssikkerhedsansvar. 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 - Kortlagt til funktionsadskillelse, godkendelse af rollekombination, uafhængig gennemgang, konfliktkontroller og verifikation af korrigerende handlinger for rollekonflikter. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].