					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII09					Dokumenttitel: **Politik for indsamling, brug, videregivelse og deling af personhenførbare oplysninger (PII)**						
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 / regulering	Klausul / kontrol / artikel	Anvendelighed	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumenteret operationel kontrol
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Formåls- og behandlingsregistreringer
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Sammenhæng med behandlingsgrundlag
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Ansvar for deling mellem fælles dataansvarlige
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Grænser for indsamling, behandling og minimering
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Sammenhæng med rute for overførsel
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registreringer af overførsel og videregivelse
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Databehandlerinstrukser og registreringer
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Databehandlerens sammenhæng med rute for overførsel
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Databehandlerens registreringer af videregivelser og anmodninger
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Formålsbegrænsning, dataminimering og ansvarlighed
GDPR	Article 6	Controller	Referenced	Sammenhæng med behandlingsgrundlag
GDPR	Article 24	Controller	Supporting	Den dataansvarliges ansvar
GDPR	Article 26	Joint Controller	Supporting	Ordninger mellem fælles dataansvarlige
GDPR	Article 28	Both	Supporting	Databehandlerinstrukser og grænser for videregivelse

GDPR	Article 30	Both	Supporting	Registreringer af behandling og modtagere
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Formåls-, indsamlings-, minimerings- og videregivelsesbegrænsning
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Ansvarlighed og efterlevelse af databeskyttelse
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Kontroller for formål, indsamling, minimering, brug og videregivelse

1. Omfang

1.1 Denne politik fastsætter krav til indsamling, brug, videregivelse og deling af PII inden for PIMS-omfanget.

1.2 Denne politik gælder for:

1.2.1 indsamling af PII via direkte, indirekte, automatiserede, manuelle, interne, eksterne og tredjepartskanaler;

1.2.2 godkendt intern brug af PII i forretningsprocesser, systemer og applikationer;

1.2.3 viderebehandling af PII til et nyt eller væsentligt ændret formål;

1.2.4 ekstern videregivelse af PII til modtagere, partnere, myndigheder, databehandlere, underdatabehandlere, leverandører og andre tredjeparter;

1.2.5 tilbagevendende datadelingsordninger og enkeltstående videregivelser;

1.2.6 kontekster som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler;

1.2.7 REG02 - fortegnelse over behandling af PII / ROPA, REG08 - register over databehandlere, underdatabehandlere og datadeling, REG09 - register over internationale overførsler, og REG12 - register over revision, afvigelser, korrigerende handlinger og forbedringer.

1.3 Denne politik erstatter ikke:

1.3.1 PII03 for fortegnelse over behandlingsaktiviteter, behandlingsgrundlag og ejerskab af ROPA;

1.3.2 PII04 for indhold, offentliggørelse og versionsstyring af privatlivsmeddelelser;

1.3.3 PII05 for håndtering af samtykke og præferencer;

1.3.4 PII06 for håndtering af rettighedsanmodninger fra registrerede;

1.3.5 PII07 for DPIA-metodik og risikovurdering vedrørende databeskyttelse;

1.3.6 PII08 for kontrolporte for databeskyttelse gennem design;

1.3.7 PII10 for udførelse af opbevaring, sletning og bortskaffelse;

1.3.8 PII11 for styring af nøjagtighed og kvalitet;

1.3.9 PII12 for livscyklusgovernance for databehandlere, underdatabehandlere og tredjeparter;

1.3.10 PII13 for valg af mekanisme til international overførsel og kontroller for overførselsrisici;

1.3.11 PII14 for PII-sikkerhed og adgangsstyring;

1.3.12 PII15 for håndtering af hændelser og brud;

1.3.13 PII18 for PIMS-dækkende governance for overvågning, revision, afvigelser, korrigerende handlinger og forbedringer.

1.4 I denne politik gælder følgende:

1.4.1 "godkendt brug" betyder en brug af PII, der er registreret i REG02 for en bestemt behandlingsaktivitet, et bestemt formål, en PII-kategori, en kategori af registrerede, en forretningsansvarlig og en relevant PIMS-rolle.

1.4.2 "indsamling" betyder indhentning af PII direkte fra en registreret, indirekte fra en anden part, automatisk fra et system eller en enhed eller via en intern eller ekstern datakilde.

1.4.3 "viderebehandling" betyder brug af PII til et formål, der ikke allerede er registreret som et godkendt formål i REG02 for den relevante behandlingsaktivitet.

1.4.4 "forenelighedsvurdering" betyder en dokumenteret vurdering i REG02 af det oprindelige formål, det foreslåede formål, afhængighed af behandlingsgrundlag, PII-kategorier,

forventninger hos registrerede, begrundelse for minimering, påvirkning af videregivelse eller overførsel samt henvisning til andre PIMS-politikker, hvor det er nødvendigt.

1.4.5 "ekstern videregivelse" betyder at gøre PII tilgængelige for en part uden for organisationen eller uden for den dokumenterede kæde af kundens instrukser.

1.4.6 "datadeling" betyder en tilbagevendende eller struktureret ordning, hvorunder PII videregives, overføres, tilgås, udveksles eller gøres tilgængelige for en anden part.

1.4.7 "følsom tilbagevendende deling" betyder tilbagevendende deling, der omfatter særlige kategorier af personoplysninger, oplysninger om straffedomme og lovovertrædelser, PII om børn, registreringer med høj påvirkning, deling i stor skala eller ekstern deling, der omfatter en overførselslokation registreret i REG09.

2. Formål

2.1 Formålet med denne politik er at sikre, at PII kun indsamles, bruges, videregives og deles til dokumenterede, godkendte, begrænsede og ansvarlige formål.

2.2 Denne politik gør det muligt for organisationen at dokumentere, at indsamling og brug er knyttet til behandlingsregistreringer i REG02, at videregivelser og datadelingsordninger registreres i REG08, at rute for international overførsel er knyttet til REG09, og at undtagelser og afvigelser håndteres via REG12.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 begrænse indsamling til PII, der er nødvendige for dokumenterede formål;

3.1.2 sikre, at intern brug af PII er godkendt, før behandling påbegyndes;

3.1.3 kræve forenelighedsvurderinger før viderebehandling;

3.1.4 kræve godkendelse og dokumentation før ekstern videregivelse;

3.1.5 opretholde dokumentation for datadeling i REG08 uden at oprette et særskilt datadelingsregister;

3.1.6 henvise afhængigheder ved international overførsel til REG09 og PII13 uden at duplikere kontroller for overførselsmekanismer;

3.1.7 definere gennemgangsfrekvens for tilbagevendende deling;

3.1.8 opretholde revisionsklart bevismateriale for indsamling, brug, videregivelse, deling, undtagelser og korrigerende handlinger.

4. Politikkerklæringer

4.1 Begrænsning af indsamling

4.1.1 [Controller] Process Owner / Business Owner skal registrere indsamlingsformål, kilde eller kanal, PII-kategorier, kategorier af registrerede og minimumsdataelementer i REG02, før en ny indsamlingsaktivitet eller væsentlig ændring af indsamling påbegyndes.

4.1.2 [Controller] Privacy Lead / PIMS Manager skal gennemgå indsamlingsregistreringen i REG02, før indsamling påbegyndes, når en ny PII-kategori, kilde, kanal eller et nyt formål tilføjes.

4.1.3 [Controller] Process Owner / Business Owner skal registrere en nødvendighedsbegrundelse i REG02 for hvert PII-dataelement, før dette element indsamles.

4.1.4 [Processor] Process Owner / Business Owner skal registrere referencen til kundens instruks fra REG08 i REG02, før PII indsamles på vegne af en kunde.

4.1.5 [Joint Controller] Process Owner / Business Owner skal registrere ansvarsfordelingen for indsamling mellem fælles dataansvarlige i REG08, før fælles indsamling påbegyndes.

4.2 Kontroller for godkendt intern brug

4.2.1 [Controller] Process Owner / Business Owner skal registrere regler for godkendt intern brug for hver behandlingsaktivitet i REG02, før brugen påbegyndes.

4.2.2 [Controller] System Owner / Application Owner skal kun implementere workflowfelter, rapporter eller eksporter til intern brug, der har en tilsvarende regel for godkendt brug i REG02, før frigivelse til produktion.

4.2.3 [Processor] Process Owner / Business Owner skal registrere overensstemmelse med kundens instruks i REG08, før kundens PII bruges til en databehandler- eller underdatabehandleraktivitet.

4.2.4 [Controller] Privacy Lead / PIMS Manager skal gennemgå regler for godkendt brug i REG02 mindst årligt for hver aktiv behandlingsaktivitet.

4.2.5 [All] Privacy Lead / PIMS Manager skal registrere en afvigelse i REG12 inden for fem arbejdsdage, når udokumenteret intern brug af PII identificeres.

[... 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 registrere en undtagelsesanmodning i REG12, før der afviges fra en godkendt regel for indsamling, brug, videregivelse eller deling.

9.1.2 [All] Privacy Lead / PIMS Manager skal registrere en beslutning om godkendelse eller afvisning i REG12, før en undtagelse aktiveres.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG12 før godkendelse af en undtagelse, der omfatter uforenelig viderebehandling, følsom tilbagevendende deling, konflikt ved retligt bindende videregivelse eller rute for overførsel.

9.1.4 [All] Top Management skal registrere godkendelse i REG12 før aktivering af enhver undtagelse med en varighed på mere end 30 kalenderdage eller med påvirkning af mere end én behandlingsaktivitet.

9.1.5 [All] Process Owner / Business Owner skal lukke en undtagelse i REG12 senest på udløbsdatoen eller inden for fem arbejdsdage efter, at undtagelsesbetingelsen ophører.

10. Håndhævelse

10.1.1 [All] Privacy Lead / PIMS Manager skal registrere ikke-godkendt indsamling, brug, videregivelse eller deling som en afvigelse i REG12 inden for fem arbejdsdage efter identifikation.

10.1.2 [Controller] Process Owner / Business Owner skal suspendere indsamling, brug, videregivelse eller deling inden for én arbejdsdag, når Privacy Lead / PIMS Manager registrerer fravær af godkendt REG02- eller REG08-dokumentation i REG12.

10.1.3 [Processor] Process Owner / Business Owner skal registrere en beslutning om stop eller eskalering i REG08 og REG12 inden for én arbejdsdag, når kundens PII bruges eller videregives uden for dokumenteret instruks.

10.1.4 [All] Top Management skal gennemgå uafklarede afvigelser vedrørende indsamling, brug, videregivelse eller deling med høj påvirkning i REG12 inden for 30 kalenderdage efter eskalering.

10.1.5 [All] Internal Audit / Compliance Reviewer skal verificere dokumentation for lukning af korrigerende handling i REG12 inden for 15 arbejdsdage efter, at Privacy Lead / PIMS Manager markerer lukning.

11. Gennemgang og vedligeholdelse

11.1.1 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik mindst årligt og registrere beslutningen i REG12.

11.1.2 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik inden for 30 kalenderdage efter en væsentlig ændring af PIMS-omfang, behandlingsformål, delingsmodel, overførselsrute eller relevant forpligtelse og registrere resultatet i REG12.

11.1.3 [All] Process Owner / Business Owner skal recertificere aktive REG02- og REG08-registreringer mindst årligt og inden for 30 kalenderdage efter en væsentlig behandlingsændring.

11.1.4 [All] Internal Audit / Compliance Reviewer skal medtage PII09-kontroller i årlige revisionsstikprøver og registrere dækningen i REG12.

11.1.5 [All] Privacy Lead / PIMS Manager skal opdatere relaterede politikreferencer i REG12 inden for ti arbejdsdage, når PII03, PII08, PII10, PII12, PII13, PII14 eller PII18 ændrer denne politiks operationelle afgrænsning.

12. Relaterede politikker

12.1 Denne politik bør læses sammen med:

12.1.1 PII01 - Politik for Privacy Information Management System

12.1.2 PII02 - Politik for roller, ansvar og ansvarlighed vedrørende databeskyttelse

12.1.3 PII03 - Politik for fortegnelse over behandling af PII og behandlingsgrundlag

12.1.4 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.1.5 PII05 - Politik for styring af samtykke og præferencer

12.1.6 PII06 - Politik for håndtering af registreredes rettigheder

12.1.7 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.1.8 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.1.9 PII10 - Politik for opbevaring, sletning og bortskaffelse af PII

12.1.10 PII11 - Politik for nøjagtighed og kvalitet af PII

12.1.11 PII12 - Politik for databehandleres, underdatabehandleres og tredjeparters styring af databeskyttelse

12.1.12 PII13 - Politik for international overførsel af PII

12.1.13 PII14 - Politik for PII-sikkerhed og adgangsstyring

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

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

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

13. Referencestandarder og rammeværker

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

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Kortlagt til dokumenterede operationelle registreringer og kontrol med bevismateriale for indsamling, godkendt brug, viderebehandling, videregivelse, deling og overførselsrute. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Kortlagt til overvågning, måling, gennemgang, undtagelseshåndtering, afvigelser og korrigerende handlinger for kontroller vedrørende indsamling, brug, videregivelse og deling. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Kortlagt til dokumenterede formål for dataansvarlige, registreringer af godkendt brug og behandlingsdokumentation i REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Kortlagt til sammenhæng med behandlingsgrundlag for indsamling, brug og viderebehandling uden at erstatte PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Kortlagt til dokumentation i REG08 for ansvar for indsamling og deling mellem fælles dataansvarlige. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Kortlagt til begrænsning af indsamling, begrænsning af behandling og minimeringsbegrundelse, før PII indsamles eller bruges. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Kortlagt til sammenhæng med rute for overførsel via REG09 uden at erstatte PII13-kontroller for overførselsmekanismer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Kortlagt til registreringer af overførsler, videregivelser og tilbagevendende datadelingsordninger i REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Kortlagt til overensstemmelse med kundens instruks for databehandlere og databehandlerregistreringer for grænser for indsamling, brug og viderebehandling. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Kortlagt til databehandlerens sammenhæng med rute for overførsel via REG09 uden at erstatte PII13-kontroller for overførselsmekanismer. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Kortlagt til databehandlerens registreringer af videregivelser, status for underretning om videregivelsesanmodninger og dokumentation for videregivelsesgodkendelse i REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Kortlagt til bevismateriale for formålsbegrænsning, dataminimering og ansvarlighed ved indsamling, brug, viderebehandling, videregivelse og deling. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Kortlagt til sammenhæng med behandlingsgrundlag og rute for ny eller uforenelig viderebehandling uden at erstatte PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Kortlagt til den dataansvarliges governance, godkendelser, gennemgang og ansvarlighedsforanstaltninger for indsamling, brug, videregivelse og deling. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Kortlagt til dokumentation for ansvar for indsamling og deling mellem fælles dataansvarlige. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Kortlagt til overensstemmelse med instrukser for databehandlere og underdatabehandlere, kundegodkendelse og grænser for videregivelse. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Kortlagt til registreringer af behandling, modtagere, videregivelse og deling i REG02 og REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kortlagt til formålsspecifikation, begrænsning af indsamling, dataminimering, begrænsning af brug og begrænsning af videregivelse. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Kortlagt til ansvarlighed, efterlevelsesdokumentation, gennemgang, undtagelseshåndtering, revisionsstikprøver og korrigerende handling. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Kortlagt til formål, begrænsning af indsamling, minimering, begrænsning af brug, begrænsning af videregivelse og understøttelse af registreringer af videregivelse. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].