					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII01					Dokumenttitel: **Politik for Privacy Information Management System**						
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 4.1	Both	Primary	Kontekst og fastlæggelse af PIMS-rolle
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Interessenter og krav
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS-omfang
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Etablering og forbedring af PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Lederskab og forpligtelse
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Privatlivspolitik
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Roller og beføjelser
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Risici og muligheder
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Risikovurdering vedrørende databeskyttelse
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Risikobehandling vedrørende databeskyttelse og SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Databeskyttelsesmål
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Planlagte PIMS-ændringer
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Ressourcer
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetence
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Bevidsthed
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Kommunikation
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterede oplysninger

ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operationel planlægning og styring
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operationel risikovurdering vedrørende databeskyttelse
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operationel risikobehandling vedrørende databeskyttelse
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Overvågning og evaluering
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Intern revision
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Ledelsens gennemgang
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Løbende forbedring
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Afvigelse og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Styringsregistreringer for dataansvarlig
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Databehandleraftale og formål
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Sammenhæng med politik for PII-sikkerhed
GDPR	Article 5(2)	Controller	Supporting	Bevismateriale for ansvarlighed
GDPR	Article 24	Controller	Supporting	Foranstaltninger og politik for dataansvarlig
GDPR	Article 26	Joint Controller	Supporting	Ordninger for fælles dataansvarlige
GDPR	Article 28	Both	Supporting	Styring af databehandlere
GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter
GDPR	Article 32	Both	Supporting	Behandlingssikkerhed
GDPR	Article 35	Controller	Supporting	DPIA-styring

ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Privatlivskontroller og principper
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-proces og forberedelse
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII-beskyttelsesprogram og politik
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integration af organisatorisk privatlivsrisiko

1. Omfang

1.1 Denne politik etablerer organisationens Privacy Information Management System for behandling af PII i sammenhænge som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler.

1.2 Denne politik gælder for:

1.2.1 PIMS-omfang, kontekst, interessenter og organisatoriske afgrænsninger;

1.2.2 fastlæggelse af PIMS-rolle for PII-behandlingsaktiviteter;

1.2.3 privatlivspolitik, databeskyttelsesmål, risikovurdering vedrørende databeskyttelse, risikobehandling vedrørende databeskyttelse og PIMS-anvendelseserklæring;

1.2.4 PIMS-styring, overvågning, intern revision, ledelsens gennemgang, afvigelse, korrigerende handling og løbende forbedring;

1.2.5 dokumenterede oplysninger og bevismateriale, der er nødvendige for at dokumentere PIMS-overensstemmelse og ansvarlighed.

1.3 I denne politik betyder en væsentlig ændring enhver ændring, der påvirker PIMS-omfang, PII-behandlingsformål, PII-kategorier, kategorier af registrerede, behandlingslokationer, rollefordeling som dataansvarlig eller databehandler, systemarkitektur, leverandør- eller underdatabehandlerordninger, privatlivsrisikoprofil, gældende retlige eller kontraktlige forpligtelser eller certificeringsomfang.

2. Formål

2.1 Denne politik definerer de obligatoriske styringskrav for etablering, implementering, vedligeholdelse, overvågning og løbende forbedring af PIMS.

2.2 Formålet med denne politik er at sikre, at organisationen kan dokumentere ansvarlig, risikobaseret og evidensdrevet styring af PII-behandling på tværs af gældende PIMS-roller.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 definere PIMS-omfang, kontekst, afgrænsninger og rolleanvendelighed;

3.1.2 tildele styringsmæssig ansvarlighed for PIMS ved brug af kanoniske PIMS-roller;

3.1.3 etablere databeskyttelsesmål og målbare forventninger til PIMS-præstation;

3.1.4 vedligeholde en PIMS-anvendelseserklæring for valgte og fravalgte kontroller;

3.1.5 integrere risikovurdering vedrørende databeskyttelse, risikobehandling vedrørende databeskyttelse og DPIA-styring i PIMS-driften;

3.1.6 sikre, at forpligtelser som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler er identificeret, før behandling påbegyndes;

3.1.7 vedligeholde revisionsklart bevismateriale til certificeringsberedskab og løbende forbedring;

3.1.8 undgå unødvendige roller, registre, formularer og overlappende operationelle kontroller.

4. Politikkerklæringer

4.1 Etablering, kontekst og omfang for PIMS

4.1.1 [Both] Top Management MUST godkende PIMS-omfanget i REG01 før den indledende PIMS-implementering og senest 30 dage efter enhver væsentlig ændring.

4.1.2 [Both] Privacy Lead / PIMS Manager MUST dokumentere eksterne og interne kontekstforhold vedrørende databeskyttelse i REG01 årligt og senest 30 dage efter enhver væsentlig ændring.

4.1.3 [Both] Privacy Lead / PIMS Manager MUST dokumentere relevante interessenter og deres PIMS-krav i REG01 årligt og senest 30 dage efter enhver væsentlig ændring.

4.1.4 [Both] Privacy Lead / PIMS Manager MUST vedligeholde oversigten over PIMS-procesinteraktioner i REG01 før hver ledelsens gennemgang.

4.2 Fastlæggelse af PIMS-rolle

4.2.1 [Both] Process Owner / Business Owner MUST klassificere organisationens PIMS-rolle for hver PII-behandlingsaktivitet i REG02, før behandlingsaktiviteten påbegyndes.

4.2.2 [Joint Controller] Vendor / Procurement Owner MUST dokumentere ansvarsfordelingen mellem fælles dataansvarlige i REG08, før fælles behandling påbegyndes.

4.2.3 [Processor] Vendor / Procurement Owner MUST dokumentere kundens behandlingsinstrukser for databehandleraktiviteter i REG08 før onboarding af tjenesten.

4.2.4 [Subprocessor] Vendor / Procurement Owner MUST dokumentere upstream-kundeinstrukser og godkendte underdatabehandlerordninger i REG08, før underdatabehandling påbegyndes.

[... 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 Anmodning om og godkendelse af undtagelse

9.1.1 [All] Process Owner / Business Owner MUST dokumentere enhver anmodet undtagelse fra denne politik i REG12, før afvigelsen finder sted.

9.1.2 [Both] Privacy Lead / PIMS Manager MUST vurdere privatlivsrisikoen ved hver anmodet undtagelse i REG04 før godkendelse.

9.1.3 [Both] Top Management MUST godkende undtagelser, der overstiger accepterede privatlivsrisikotærskler, i REG12 før implementering.

9.1.4 [Both] Privacy Lead / PIMS Manager MUST gennemgå aktive PIMS-undtagelser i REG12 kvartalsvist indtil lukning.

9.2 Lukning af undtagelser

9.2.1 [All] Process Owner / Business Owner MUST dokumentere bevismateriale for lukning af undtagelse i REG12 senest på den godkendte udløbsdato for undtagelsen.

9.2.2 [Both] Internal Audit / Compliance Reviewer MUST verificere bevismateriale for lukning af udløbne undtagelser i REG12 under den næste planlagte interne revision.

10. Håndhævelse

10.1 Håndtering af afvigelser

10.1.1 [All] Privacy Lead / PIMS Manager MUST registrere formodede afvigelser fra denne politik i REG12 senest fem arbejdsdage efter identifikation.

10.1.2 [All] Process Owner / Business Owner MUST implementere godkendte korrigerende handlinger i REG12 senest på den tildelte forfaldsdato efter godkendelse af afvigelsen.

10.1.3 [All] Top Management MUST gennemgå uløste større PIMS-afvigelser i REG12 ved hver ledelsens gennemgang.

10.1.4 [All] Internal Audit / Compliance Reviewer MUST verificere effektiviteten af korrigerende handlinger i REG12 senest 30 dage efter rapporteret lukning.

10.2 Eskalering

10.2.1 [All] Privacy Lead / PIMS Manager MUST eskalere forfaldne større korrigerende handlinger til Top Management i REG12 senest fem arbejdsdage efter forfaldsdatoen.

10.2.2 [All] Top Management MUST registrere beslutninger om forfaldne større korrigerende handlinger i REG12 senest 15 arbejdsdage efter eskalering.

11. Gennemgang og vedligeholdelse

11.1 Gennemgang af politikken

11.1.1 [All] Privacy Lead / PIMS Manager MUST gennemgå denne politik i REG12 årligt og senest 30 dage efter enhver væsentlig ændring af retlige, organisatoriske, behandlingsmæssige, teknologiske forhold eller certificeringsomfang.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUST give dokumenteret rådgivning i REG12 før godkendelse af politikken, når væsentlige databeskyttelsesforpligtelser ændres.

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

11.1.4 [All] Privacy Lead / PIMS Manager MUST opdatere REG01 og REG03 senest 15 arbejdsdage efter godkendte politikændringer, der ændrer PIMS-omfang eller kontrolanvendelighed.

11.1.5 [All] Privacy Lead / PIMS Manager MUST registrere kommunikation af godkendte politikændringer i REG11 senest 30 dage efter offentliggørelse.

12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII02 - Politik for privatlivsroller, ansvar og ansvarlighed

12.3 PII03 - Politik for PII-behandlingsfortegnelse 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 databehandlere, underdatabehandlere og datadeling

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 privatlivstræning, bevidsthed og kompetence

12.10 PII17 - Politik for PIMS-dokumenterede oplysninger og styring af bevismateriale

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

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 organisatorisk kontekst, kontekstforhold vedrørende databeskyttelse og anvendelighed af roller som dataansvarlig eller databehandler for PIMS-aktiviteter. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Kortlagt til identifikation af interessenter, registrerede, kunder, tilsynsmyndigheder, databehandlere, underdatabehandlere og deres relevante PIMS-krav. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Kortlagt til definition, godkendelse, vedligeholdelse og ændring af det dokumenterede PIMS-omfang. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Kortlagt til etablering, implementering, vedligeholdelse og forbedring af PIMS-processer og deres indbyrdes samspil. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Kortlagt til Top Management-godkendelse, ressourcer, styringsgennemgang og lederskab vedrørende PIMS-effektivitet og forbedring. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Kortlagt til vedligeholdelse af denne privatlivspolitik som godkendte dokumenterede oplysninger og kommunikation af politikændringer. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Kortlagt til tildeling og kommunikation af PIMS-roller, ansvar og beføjelser. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Kortlagt til planlægning af handlinger for PIMS-risici og muligheder med brug af kontekst, interessentkrav, mål og input til forbedring. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Kortlagt til krav om risikovurdering vedrørende databeskyttelse før ny eller væsentligt ændret behandling og vedligeholdelse af bevismateriale for privatlivsrisiko. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Kortlagt til risikobehandling vedrørende databeskyttelse, valg af kontroller, sammenhæng med informationssikkerhedsprogram og vedligeholdelse af anvendelseserklæring. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Kortlagt til etablering, måling, overvågning, kommunikation og opdatering af PIMS-mål. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Kortlagt til planlagte PIMS-ændringer og styring af ændringer, der påvirker omfang, roller, kontroller og dokumenterede oplysninger. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Kortlagt til fastlæggelse og tilvejebringelse af ressourcer til etablering, drift, vedligeholdelse og forbedring af PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Kortlagt til kompetenceforventninger og bevismateriale, der understøtter PIMS-ansvar og rolleudførelse. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Kortlagt til bevidsthed om privatlivspolitikken, bidrag til PIMS-effektivitet og konsekvenser af afvigelser. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Kortlagt til intern og ekstern kommunikation, der er relevant for PIMS-styring, politikændringer og eskalering. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Kortlagt til oprettelse, vedligeholdelse, styring, klargøring af bevismateriale og opbevaring af dokumenterede oplysninger. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Kortlagt til planlægning, implementering og styring af PIMS-driftsprocesser og eksternt leverede processer. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Kortlagt til gennemførelse af risikovurderinger vedrørende databeskyttelse med planlagte intervaller, og når væsentlige ændringer foreslås eller indtræffer. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Kortlagt til implementering af planer for risikobehandling vedrørende databeskyttelse og opbevaring af bevismateriale for behandlingsresultater. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Kortlagt til overvågning, måling, analyse, evaluering, metrikker og rapportering om PIMS-effektivitet. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Kortlagt til planlægning af intern revision, stikprøver af bevismateriale, revisionsresultater og uafhængig gennemgang. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Kortlagt til input til ledelsens gennemgang, gennemgang af præstation, output fra ledelsens gennemgang og forbedringsbeslutninger. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Kortlagt til løbende forbedring gennem ledelsens gennemgang, metrikker, opfølgning på korrigerende handlinger og vedligeholdelse af politikken. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Kortlagt til håndtering af afvigelser, korrigerende handling, eskalering, lukning og verifikation af effektivitet. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Kortlagt til registreringer på dataansvarligsiden om behandlingsformål, sammenhæng med behandlingsgrundlag, afgørelse af DPIA-behov, ansvarsfordeling mellem fælles dataansvarlige og bevisregistreringer for behandling. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Kortlagt til kundeaftaler for databehandlere, dokumenterede kundeinstrukser og formålsbegrænsninger for databehandlere. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Kortlagt til sammenhæng med PII-sikkerhedspolitik, ejerskab af baseline for PII-sikkerhedskontroller og status for informationssikkerhedskontroller i PIMS-anvendelseserklæringen. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Kortlagt til bevismateriale for ansvarlighed, godkendelse af politik, klassificering af behandlingsrolle, kontrolanvendelighed, overvågning, revision og registreringer af korrigerende handlinger. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Kortlagt til styringsforanstaltninger for dataansvarlige, godkendelse af politik, PIMS-mål, gennemgang af effektivitet og dokumenteret bevismateriale for dataansvarliges ansvarlighed. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Kortlagt til fastlæggelse og dokumentation af ansvarsfordeling mellem fælles dataansvarlige, før fælles behandling påbegyndes. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Kortlagt til styringsregistreringer for databehandlere og underdatabehandlere, kundens behandlingsinstrukser og styring af eksternt leverede processer. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Kortlagt til registreringer af behandlingsaktiviteter, rolleklassificering, ansvarlighedsregistreringer for behandling og bevismateriale opbevaret til revisionsbarhed. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Kortlagt til styring af PII-sikkerhedsbaseline, ejerskab af sikkerhedskontroller, implementeringsstatus for sikkerhed og bekræftelse af operationelle kontroller. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Kortlagt til afgørelse af DPIA-behov og risikovurdering vedrørende databeskyttelse, før højrisikobehandling eller væsentligt ændret behandling som dataansvarlig fortsætter. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Kortlagt til identifikation af privatlivskontroller, privatlivsprincipper, informationssikkerhed, efterlevelse af

databeskyttelseskrav, revision, bevismateriale og risikobaseret styring af databeskyttelse. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Kortlagt til PIA-styring, afgørelse af DPIA-udløsere, PIA-forberedelse, kriterier for privatlivsrisiko og dokumenteret bevismateriale for risikovurdering vedrørende databeskyttelse. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Kortlagt til krav til PII-beskyttelsesprogram, identifikation af krav til PII-beskyttelse, risikobaseret valg af privatlivskontroller og politisk retning for PII-beskyttelse. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Kortlagt til organisatoriske principper for privatlivsrisiko, ledelsens forpligtelse, integration af privatlivsrisiko i PIMS-styring og forståelse af organisationens rolle i PII-behandling. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].