

				Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: PII10				Dokumenttitel: Politik for opbevaring, sletning og bortskaffelse 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

Juridisk meddelelse (ophavsret og brugsbegrænsninger)
(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.

Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.

For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard / regulering	Klausul / kontrol / artikel	Anvendelsesområde	Dækningstype	Kommentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumenteret bevismateriale for opbevaring og operationel kontrol
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Overvågning, afvigelse og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Fælles ansvar og behandlingsregistreringer
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Understøttelse af gennemførelse af sletning
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Opbevaring, sletning og bortskaffelse
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Kundeinstrukser og databehandlerregistreringer
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Understøttelse af sletning og bortskaffelseskapacitet
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Bortskaffelse af medier og håndtering af sikkerhedskopier
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Opbevaringsbegrænsning og ansvarlighed
GDPR	Article 17	Controller	Supporting	Understøttelse af gennemførelse af sletning
GDPR	Article 24	Controller	Supporting	Foranstaltninger for dataansvarlig
GDPR	Article 26	Joint Controller	Supporting	Fordeling af fælles ansvar
GDPR	Article 28	Processor	Supporting	Databehandlers sletning og tilbagelevering

GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter
GDPR	Article 32	Both	Supporting	Sikker behandling og understøttelse af bortskaffelse
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimering, opbevaringsbegrænsning og ansvarlighed
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Kontroller for opbevaring og sletning af midlertidige filer
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Sletteramme og dokumentation
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Sletteperioder og sletteregler
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Implementering og undtagelser
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Ansvar og implementeringsstyring
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integration af risici vedrørende databeskyttelse
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Sikker bortskaffelse og sletning af information

1. Omfang

- 1.1 Denne politik fastlægger organisationens krav til at definere, gennemgå, udføre og dokumentere opbevaring, sletning, anonymisering, afidentificering, tilbagelevering, overførsel og bortskaffelse af PII.
- 1.2 Denne politik gælder for PII, der behandles i roller som dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler, herunder PII i driftssystemer, arkiver, sikkerhedskopier, replikaer, logfiler, stagingmiljøer, midlertidige filer, papirregistre og lagringsmedier.
- 1.3 Denne politik gælder for opbevarings- og sletteforpligtelser, der følger af godkendte behandlingsformål, registreringer af behandlingsgrundlag, instrukser fra dataansvarlige, kontraktlige krav, udfald af sletning for registrerede, service-exit, bortskaffelse af lagringsmedier og overvågningskonstatationer i PIMS.
- 1.4 Denne politik fastlægger ikke valg af behandlingsgrundlag, indhold i privatlivsmeddelelser, fuld håndtering af registreredes rettigheder, styring af databehandleres livscyklus, mekanismer for internationale overførsler, arkitektur for sikkerhedskontroller, arbejdsgange for hændeshåndtering eller revisionsmetodik for PIMS. Disse kontroller behandles i relaterede politikker.
- 1.5 I denne politik betyder en væsentlig ændring enhver ændring af behandlingsformål, PII-kategori, kategori af registrerede, systemets lagringslokation, opbevaringslovgivning eller kontrakt, kundens instruks, backuparkitektur, arkiveringsmetode, bortskaffelsesmetode, databehandler- eller underdatabehandlerordning, slettearbejdsgang eller PIMS-certificeringsomfang, som påvirker opbevaring, sletning eller bortskaffelse.

2. Formål

- 2.1 Formålet med denne politik er at sikre, at PII kun opbevares til godkendte formål og i godkendte perioder, slettes eller på anden måde bortskaffes, når det ikke længere er nødvendigt, og understøttes af revisionsklart bevismateriale.
- 2.2 Denne politik gør organisationen i stand til at dokumentere opbevaringsbegrænsning, ansvarlig styring af opbevaring, kontrolleret gennemførelse af sletning, sikker bortskaffelse, overensstemmelse med databehandlerinstrukser, styring af undtagelser og løbende forbedring uden at oprette et særskilt sletteregister.

3. Mål

3.1 Målene med denne politik er at:

- 3.1.1 definere ejerskab for opbevaringsregler og påkrævede opbevaringsmetadata;
- 3.1.2 sikre, at opbevaringsregler registreres i fortegnelsen over PII-behandlingsaktiviteter / ROPA;
- 3.1.3 sikre, at databehandleres og underdatabehandleres slettehandlinger baseres på kundens instruks eller kontrakt;
- 3.1.4 sikre, at udløbet PII slettes, tilbageleveres, overføres, anonymiseres, afidentificeres eller bortskaffes ved brug af godkendte metoder;
- 3.1.5 skelne mellem driftssystemer, arkiver, sikkerhedskopier, replikaer, logfiler, stagingområder og midlertidige filer;
- 3.1.6 sikre, at bevismateriale for sletning og bortskaffelse opbevares i kanoniske PIMS-bevisobjekter;
- 3.1.7 sikre, at undtagelser fra opbevaring er tidsbegrænsede, godkendte og gennemgået;
- 3.1.8 integrere overvågning af opbevaring og sletning med afvigelse, korrigerende handlinger og forbedring.

4. Politikerkklæringer

4.1 Tildeling af opbevaringsregler

- 4.1.1 [Controller] Process Owner / Business Owner skal tildele en dokumenteret opbevaringsregel til hver behandlingsaktivitet som dataansvarlig i REG02, før behandlingsaktiviteten påbegyndes.
- 4.1.2 [Joint Controller] Process Owner / Business Owner skal registrere fordelingen af ansvar for opbevaring og sletning mellem fælles dataansvarlige i REG02 og REG08, før fælles behandling påbegyndes eller ændres.
- 4.1.3 [Processor] Vendor / Procurement Owner skal registrere kundens instrukser om opbevaring, tilbagelevering, overførsel eller sletning for databehandleraktiviteter i REG08, før databehandlerens behandling påbegyndes eller ændres.
- 4.1.4 [Subprocessor] Vendor / Procurement Owner skal registrere krav om videreførelse af opbevaring, tilbagelevering, overførsel eller sletning til underdatabehandler i REG08, før underdatabehandleren onboardes eller instruksen ændres.
- 4.1.5 [Both] Privacy Lead / PIMS Manager skal verificere, at hver godkendt opbevaringsregel i REG02 omfatter opbevaringsperiode, starttrigger, ejer, begrundelse, endelig håndtering og næste gennemgangsdato, før reglen godkendes.
- 4.1.6 [Both] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG02 eller REG12 før godkendelse af enhver opbevaringsregel, der omfatter juridisk konflikt, højrisikobehandling, særlige kategorier af personoplysninger eller opbevaring ud over det oprindelige behandlingsformål.

4.2 Gennemgang og begrænsning af opbevaring

- 4.2.1 [Both] Process Owner / Business Owner skal gennemgå tildelte opbevaringsregler i REG02 mindst årligt og inden for 30 dage efter en væsentlig ændring.
- 4.2.2 [Both] Privacy Lead / PIMS Manager skal godkende eller afvise nye eller ændrede opbevaringsregler i REG02 inden for 10 arbejdsdage efter indsendelse.
- 4.2.3 [Both] System Owner / Application Owner skal bekræfte den tekniske eller manuelle håndhævelsesmetode for hver opbevaringsregel i REG02 før idriftsættelse i produktionsmiljøet og ved hver årlig gennemgang af opbevaring.
- 4.2.4 [Controller] Process Owner / Business Owner skal begrænse aktiv brug af PII, der kun opbevares af juridiske, kontraktlige, revisionsmæssige eller tvistrelaterede årsager, i REG02 inden for fem arbejdsdage efter identifikation af begrænsningsbetingelsen.
- 4.2.5 [Both] Privacy Lead / PIMS Manager skal registrere uafklaret risiko for opbevaring ud over godkendte perioder eller forsinket gennemgang af opbevaring i REG12 inden for 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 indsende enhver anmodning om at opbevare PII ud over den godkendte REG02-opbevaringsregel i REG12, før undtagelsen bliver aktiv.
- 9.1.2 [All] Privacy Lead / PIMS Manager skal godkende eller afvise anmodninger om opbevaringsundtagelser i REG12, før undtagelsen bliver aktiv.
- 9.1.3 [All] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG12 før godkendelse af enhver undtagelse, der omfatter juridisk konflikt, afslag på sletning, højrisiko-PII, ekstern deling eller certificeringspåvirkning.

- 9.1.4 [All] Top Management skal godkende opbevaringsundtagelser, der overstiger 90 dage, påvirker højrisikobehandling eller påvirker ekstern assurance, i REG12, før undtagelsen bliver aktiv.
- 9.1.5 [All] Privacy Lead / PIMS Manager skal tildele ejer, udløbsdato, kompenserende kontrol og gennemgangsfrekvens i REG12 for hver godkendt undtagelse vedrørende opbevaring, sletning eller bortskaffelse.
- 9.1.6 [All] Privacy Lead / PIMS Manager skal gennemgå hver åben undtagelse i REG12 mindst månedligt indtil lukning.
- 9.1.7 [All] Process Owner / Business Owner skal lukke eller forny hver undtagelse i REG12 før undtagelsens udløbsdato.

10. Håndhævelse

- 10.1.1 [All] Privacy Lead / PIMS Manager skal registrere en afvigelse i REG12 inden for fem arbejdsdage efter identifikation af manglende opbevaringsmetadata, forsinket gennemgang af opbevaring, ikke-understøttet opbevaring, manglende handling for endelig håndtering eller manglende bevismateriale.
- 10.1.2 [All] System Owner / Application Owner skal suspendere ny produktionsbrug af en behandlingsaktivitet i REG12, når påkrævede tekniske opbevaringskontroller mangler før idriftsættelse.
- 10.1.3 [All] Process Owner / Business Owner skal standse ikke-godkendt aktiv brug af PII, der kun opbevares af juridiske, kontraktlige, revisionsmæssige eller tvistrelaterede årsager, inden for fem arbejdsdage og registrere handlingen i REG02 eller REG12.
- 10.1.4 [Processor] Vendor / Procurement Owner skal eskalere forsinkede kundestyrede handlinger for endelig håndtering i REG08 og REG12 inden for fem arbejdsdage efter overskredet kontraktlig frist.
- 10.1.5 [Subprocessor] Vendor / Procurement Owner skal eskalere manglende bevismateriale for underdatabehandlers endelige håndtering i REG08 og REG12 inden for fem arbejdsdage efter overskredet kontraktlig bevisfrist.
- 10.1.6 [All] Internal Audit / Compliance Reviewer skal verificere effektiviteten af korrigerende handlinger for afvigelser vedrørende opbevaring, sletning og bortskaffelse i REG12 ved den næste planlagte revision eller inden for 60 dage efter lukning, alt efter hvad der indtræffer først.
- 10.1.7 [Conditional] Incident Response Coordinator skal iværksætte håndtering i REG10, når en afvigelse vedrørende opbevaring, sletning eller bortskaffelse indikerer en mistænkt PII-hændelse.

11. Gennemgang og vedligeholdelse

- 11.1.1 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik årligt og registrere resultatet af gennemgangen i REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik inden for 30 dage efter en væsentlig ændring af opbevaringslovgivning, behandlingsformål, databehandlerinstruks, systemarkitektur, backuparkitektur, arkiveringsmetode, slettearbejdsgang, bortskaffelsesproces eller PIMS-certificeringskrav.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor skal gennemgå ændringer af denne politik med væsentlig betydning for databeskyttelse i REG12 før godkendelse.
- 11.1.4 [All] Top Management skal godkende væsentlige ændringer af denne politik i REG12 før offentliggørelse.
- 11.1.5 [All] Privacy Lead / PIMS Manager skal registrere kommunikation af godkendte politikændringer i REG11 inden for 30 dage efter offentliggørelse.

12. Relaterede politikker

- 12.1 Denne politik understøttes af følgende relaterede politikker:
- 12.2 PII01 - Politik for styringssystem for databeskyttelsesoplysninger
- 12.3 PII02 - Politik for databeskyttelsesroller, ansvar og ansvarlighed
- 12.4 PII03 - Politik for fortegnelse over PII-behandling og behandlingsgrundlag
- 12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed
- 12.6 PII06 - Politik for håndtering af registreredes rettigheder
- 12.7 PII08 - Politik for databeskyttelse gennem design og standardindstillinger
- 12.8 PII09 - Politik for indsamling, brug, videregivelse og deling af PII
- 12.9 PII12 - Politik for styring af databeskyttelse hos databehandlere, underdatabehandlere og tredjeparter
- 12.10 PII14 - Politik for PII-sikkerhed og adgangsstyring
- 12.11 PII15 - Politik for PII-hændelser og brud
- 12.12 PII17 - Politik for dokumenteret information og styring af bevismateriale i PIMS
- 12.13 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 7.5; Clause 8.1** - Kortlagt til dokumenteret bevismateriale for opbevaring, operationel planlægning, opbevaringsmetadata, implementeringsbevismateriale og registreringer af livscyklusgennemførelse. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].
- 13.2.2 **Clause 9.1; Clause 10.2** - Kortlagt til overvågning, metrikker, gennemgang af forsinkede handlinger, afvigelser og korrigerende handlinger for kontroller vedrørende opbevaring, sletning og bortskaffelse. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].
- 13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Kortlagt til bevismateriale for fælles dataansvarliges ansvar og den dataansvarliges behandlingsregistreringer, der indeholder metadata om opbevaring og endelig håndtering. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].
- 13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Kortlagt til understøttelse af gennemførelse af sletning, routing af slettevurdering og sammenkædning med tredjeparts bevismateriale, hvor sletteudfald kræver handling. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].
- 13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Kortlagt til sletning eller afidentificering ved behandlingens ophør, håndtering af midlertidige filer, opbevaringsbegrænsning og dokumenterede kontroller for endelig håndtering. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Kortlagt til databehandlers kundeaftaler, dokumenterede kundeformål og databehandlers behandlingsregistreringer. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].
- 13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Kortlagt til databehandlers understøttelse af kundens forpligtelser, håndtering af midlertidige filer og kapacitet til tilbagelevering,

overførsel eller endelig håndtering. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Kortlagt til livscyklushåndtering af lagringsmedier, kontroller ved genbrug eller frigivelse af udstyr og håndtering af sikkerhedskopier for PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Kortlagt til opbevaringsbegrænsning, ansvarlighed for opbevaring, godkendte opbevaringsmetadata, bevismateriale og gennemgang. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Kortlagt til godkendt routing af sletteudfald, bevismateriale for gennemførelse og hændelseseskalering, hvor svigt i slettekontroller indikerer en mistænkt PII-hændelse. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Kortlagt til styring for dataansvarlige, ansvarlighedsforanstaltninger, gennemgange, undtagelser, korrigerende handlinger og vedligeholdelse af politikken. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Kortlagt til fordeling af ansvar for opbevaring og sletning mellem fælles dataansvarlige. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Kortlagt til overensstemmelse med instrukser for databehandlere og underdatabehandlere, tilbagelevering, overførsel, endelig håndtering, bevismateriale og eskalering. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Kortlagt til metadata om opbevaring og endelig håndtering i behandlingsregistreringer for aktiviteter som dataansvarlig og databehandler. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Kortlagt til sikker operationel håndtering af opbevaret PII, teknisk håndhævelse, kontrol med lagringsmedier, håndtering af sikkerhedskopier og hændelseseskalering. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Kortlagt til dataminimering, begrænsning af brug og opbevaring, endelig håndtering, når oplysninger ikke længere er nødvendige, begrænsning af opbevaret PII og bevismateriale for ansvarlighed. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Kortlagt til tidsbegrænset opbevaring, endelig håndtering, automatiseret eller manuel håndhævelse og håndtering af midlertidige filer. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Kortlagt til styring af sletteramme, gruppering af PII, opbevarings- og sletteperioder, sontring mellem arkiver og sikkerhedskopier, struktur for sletteregler og krav til dokumenterede procedurer. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Kortlagt til angivelse af regelmæssige sletteperioder, identifikation af standardiserede sletteperioder og tildeling af sletteregler til PII-behandlingsaktiviteter. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Kortlagt til implementeringskrav for systemer, manuelle processer, organisationsdækkende

forhold, databehandlere, håndtering af gendannelse og undtagelsesstyring. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Kortlagt til rolletildeling, dokumentation, operationel indlejring, revision og implementeringsstyring for opbevaring, sletning og bortskaffelse. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Kortlagt til risikobaseret styring af databeskyttelse, ledelsesbevidsthed, integration af risici vedrørende databeskyttelse i PIMS og opbevaringsrelateret risikokontekst. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Kortlagt til sletning af information, kontrolleret afslutning af livscyklus, frigivelse af lagringsmedier og bevismateriale for endelig håndtering. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].