					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII08					Dokumenttitel: **Politik for databeskyttelse gennem design og standardindstillinger**						
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 6.1.2; Clause 6.1.3	Both	Supporting	Kobling til risikovurdering vedrørende databeskyttelse og risikobehandling
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Planlagte ændringer og operationel styring
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentation for databeskyttelse gennem design
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Formål, PIA-udløser og registreringer
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Begrænsning af indsamling og behandling
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Mål for korrekthed og minimering
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Design for afidentificering, sletning og midlertidige filer
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Kundeaftale, support og databehandlerregistreringer
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Databehandlerens designkapaciteter
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Udviklingslivscyklus og tekniske principper
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Formålsbegrænsning, minimering og ansvarlighed
GDPR	Article 24	Controller	Supporting	Foranstaltninger hos den dataansvarlige
GDPR	Article 25	Controller	Primary	Databeskyttelse gennem design og standardindstillinger
GDPR	Article 28	Both	Supporting	Databehandlerinstrukser og bistand
GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter

GDPR	Article 35	Controller	Supporting	Kobling til DPIA-udløser
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Privatlivskontroller gennem design
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Formål, indsamling, minimering og begrænsning af brug
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Korrekthed, ansvarlighed og efterlevelse
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Principper og kontroller for beskyttelse af PII

1. Omfang

1.1 Denne politik fastsætter krav til indbygning af databeskyttelse gennem design og databeskyttelse som standard i nye og ændrede behandlingsaktiviteter, projekter, produkter, tjenester, systemer, applikationer, integrationer, indkøbsaktiviteter og ændringer af forretningsprocesser inden for PIMS-omfanget, som omfatter PII.

1.2 Denne politik gælder i kontekster med dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler. Forpligtelser for databehandlere og underdatabehandlere gælder, hvor organisationen designer, konfigurerer, ændrer eller driver behandling på vegne af en kunde, dataansvarlig eller overordnet databehandler efter dokumenterede instrukser.

1.3 Denne politik omfatter:

1.3.1 krav til databeskyttelse ved projektopstart;

1.3.2 designkontroller for formål, dataminimering og standardindstillinger;

1.3.3 gennemgang af databeskyttelse gennem design før idriftsættelse i produktionsmiljøet;

1.3.4 ændringsudløst gennemgang af databeskyttelse gennem design;

1.3.5 kontroller af databeskyttelse gennem design ved indkøb;

1.3.6 kobling til dokumentation for databeskyttelsesrisiko, DPIA-screening og korrigerende handling.

1.4 Denne politik erstatter ikke:

1.4.1 PII03 vedrørende fortegnelse over behandlingsaktiviteter, formål, behandlingsgrundlag og ROPA-registreringer;

1.4.2 PII04 vedrørende indhold og offentliggørelse af privatlivsmeddelelse;

1.4.3 PII05 vedrørende kontroller for samtykke og præferencer;

1.4.4 PII06 vedrørende håndtering af registreredes rettigheder;

1.4.5 PII07 vedrørende metode for risikovurdering vedrørende databeskyttelse og DPIA;

1.4.6 PII09 vedrørende kontroller for indsamling, brug, videregivelse og deling;

1.4.7 PII10 vedrørende udførelse af opbevaring, sletning og bortskaffelse;

1.4.8 PII11 vedrørende drift af korrekthed og kvalitet;

1.4.9 PII12 vedrørende livscyklusstyring for databehandlere, underdatabehandlere og tredjeparter;

1.4.10 PII13 vedrørende mekanismer for international overførsel;

1.4.11 PII14 vedrørende PII-sikkerhed og drift af adgangsstyring;

1.4.12 PII18 vedrørende PIMS-dækkende overvågning, revision, korrigerende handling og forbedringsstyring.

2. Formål

2.1 Formålet med denne politik er at sikre, at krav til databeskyttelse identificeres, implementeres og dokumenteres, før behandling af PII påbegyndes eller ændres væsentligt, og at systemer og processer som standard konfigureres til at begrænse indsamling, brug, eksponering, opbevaringsafhængighed, videregivelsesafhængighed og identificerbarhed af PII til det, der er nødvendigt for det dokumenterede formål.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 indarbejde krav til databeskyttelse i beslutninger om projektopstart, design, indkøb, ændringer og idriftsættelse i produktionsmiljøet;

3.1.2 sikre, at design af behandling af PII er knyttet til dokumenterede formål og REG02-behandlingsregistreringer;

3.1.3 implementere dataminimering og standardindstillinger, der beskytter privatlivet, før behandling påbegyndes;

3.1.4 sikre, at databeskyttelsesrisiko og DPIA-screening udløses uden at duplikere PII07-metoden;

3.1.5 sikre, at krav til indkøb og databehandlerdesign registreres uden at duplikere PII12-livscyklusstyring;

3.1.6 sikre, at uløste designforhold eskaleres via REG12;

3.1.7 opretholde revisionsklar dokumentation for databeskyttelse gennem design i REG02, REG04, REG08 og REG12.

4. Politikudsagn

4.1 Projektopstart og krav til databeskyttelse

4.1.1 [Both] Process Owner / Business Owner skal registrere en post om databeskyttelse gennem design i REG04, før der igangsættes et projekt, produkt, tjeneste, system, applikation, integration eller ændring af forretningsproces, der omfatter PII.

4.1.2 [Both] Process Owner / Business Owner skal knytte hver post om databeskyttelse gennem design i REG04 til en eksisterende eller udkastet REG02-behandlingsaktivitet, før funktionelle krav godkendes.

4.1.3 [Controller] Privacy Lead / PIMS Manager skal registrere krav til databeskyttelse gennem design for den dataansvarlige i REG04, før den dataansvarliges funktionelle design godkendes.

4.1.4 [Processor] Vendor / Procurement Owner skal registrere kundens instrukser om databeskyttelse gennem design og kontraktlige designbegrænsninger i REG08, før design af databehandlertjenester eller væsentlige ændringer af tjenesten godkendes.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG04 før godkendelse af et højrisiko-, nyt, følsomt, automatiseret, storskala eller væsentligt ændret PII-design.

4.1.6 [Both] Information Security Lead skal registrere afhængigheder af PII-sikkerhedskontroller, der understøtter designet for databeskyttelse gennem design, i REG04 før arkitekturgodkendelse.

4.2 Dataminimering og design af databeskyttelse som standard

4.2.1 [Controller] Process Owner / Business Owner skal dokumentere de minimale PII-kategorier, kategorier af registrerede, kilder og formål i REG02 og REG04, før design for indsamling eller import godkendes.

4.2.2 [Both] System Owner / Application Owner skal konfigurere standardindstillinger for behandling til den minimale indsamling og behandling af PII, der er nødvendig for det dokumenterede formål, og registrere dokumentation i REG04 før idriftsættelse i produktionsmiljøet.

4.2.3 [Controller] Process Owner / Business Owner skal dokumentere valgfrie PII-felter, valgfrie behandlingsvalg og standardindstillinger, der er slået fra, i REG02 og REG04, før brugergrænseflade, formular eller arbejdsgang godkendes.

4.2.4 [Both] System Owner / Application Owner skal dokumentere standardindstillinger for privatlivseksponering for visninger, rapporter, eksporter, grænseflader og automatiserede arbejdsgange i REG04 før idriftsættelse i produktionsmiljøet.

4.2.5 [Both] Process Owner / Business Owner skal dokumentere gennemførligheden af afidentificering, pseudonymisering, aggregering eller ikke-identificerbar behandling i REG04, før identificerbar PII godkendes til test, analyse, rapportering eller sekundær driftsmæssig brug.

4.2.6 [Both] System Owner / Application Owner skal dokumentere håndtering af midlertidige PII-artefakter, herunder midlertidige filer, caches, logfiler eller stagingregistreringer, i REG04 før idriftsættelse i produktionsmiljøet.

4.2.7 [Both] Process Owner / Business Owner skal dirigere designkrav, der ejes af PII10, PII11, PII13 eller PII14, til den relaterede dokumentationsvej for politikken i REG04 senest fem arbejdsdage efter identifikation af afhængigheden.

[... 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 Undtagelser vedrørende databeskyttelse gennem design

9.1.1 [Both] Process Owner / Business Owner skal anmode om en undtagelse vedrørende databeskyttelse gennem design i REG12, før et design eller en ændring godkendes, som ikke kan opfylde et gældende krav til databeskyttelse gennem design.

9.1.2 [Both] Privacy Lead / PIMS Manager skal vurdere konsekvensen, kompenserende kontroller og udløb for hver undtagelse vedrørende databeskyttelse gennem design i REG12 senest fem arbejdsdage efter anmodning.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG12 før godkendelse af en undtagelse vedrørende databeskyttelse gennem design, der omfatter højrisiko-, følsom, automatiseret, storskala, omtvistet eller juridisk væsentlig behandling.

9.1.4 [All] Top Management skal godkende en undtagelse vedrørende databeskyttelse gennem design, der påvirker behandling med høj konsekvens, certificeringsomfang, uløst væsentlig risiko eller retlig forpligtelse, i REG12, før undtagelsen træder i kraft.

9.1.5 [Both] Privacy Lead / PIMS Manager skal fastsætte en udløbsdato på højst 90 dage i REG12 for hver godkendt undtagelse vedrørende databeskyttelse gennem design før godkendelse.

9.1.6 [Both] Privacy Lead / PIMS Manager skal lukke eller revurdere hver undtagelse vedrørende databeskyttelse gennem design i REG12 senest fem arbejdsdage efter udløb.

10. Håndhævelse

10.1 Håndhævelse og håndtering af afvigelser

10.1.1 [Both] Privacy Lead / PIMS Manager skal registrere manglende gennemgang af databeskyttelse gennem design, manglende minimeringsdokumentation, uløst svigt i standardindstillinger eller uautoriseret idriftsættelse som en afvigelse i REG12 senest fem arbejdsdage efter identifikation.

10.1.2 [Both] System Owner / Application Owner skal forhindre idriftsættelse i produktionsmiljøet af et system, der behandler PII, hvor REG04-gennemgang af databeskyttelse gennem design er ufuldstændig, og registrere beslutningen i REG12 før idriftsættelse i produktionsmiljøet.

10.1.3 [Both] Vendor / Procurement Owner skal forhindre onboarding af leverandør eller kontraktunderskrift, hvor krævet REG08-dokumentation for databeskyttelse gennem design mangler, og registrere beslutningen i REG12 før onboarding eller underskrift.

10.1.4 [Both] Process Owner / Business Owner skal suspendere brugen af et nyt eller ændret design for behandling af PII, indtil REG04-gennemgang, REG02-opdateringer og krævede REG12-undtagelser er fuldført.

10.1.5 [All] Top Management skal kræve korrigerende handling i REG12 senest 10 arbejdsdage ved gentagne, langvarige eller højkonsekvente svigt i databeskyttelse gennem design.

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

11. Gennemgang og vedligeholdelse

11.1 Gennemgang af politik og designkontroller

11.1.1 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik i REG12 årligt og senest 30 dage efter en væsentlig ændring af retlige forhold, behandling, teknologi, certificeringsomfang eller PIMS-kontroller.

11.1.2 [Both] Process Owner / Business Owner skal gennemgå aktive REG02-behandlingsaktiviteter for ændringer i afhængigheder vedrørende databeskyttelse gennem design årligt og senest 30 dage efter en væsentlig behandlingsændring.

11.1.3 [Both] System Owner / Application Owner skal gennemgå dokumentation for standardkonfiguration for databeskyttelse i REG04 årligt og senest 30 dage efter en væsentlig systemændring.

11.1.4 [Both] Vendor / Procurement Owner skal gennemgå leverandørers, databehandleres, underdatabehandleres og tredjeparters forpligtelser vedrørende databeskyttelse gennem design i REG08 før fornyelse og senest 30 dage efter en væsentlig ændring af relationen.

11.1.5 [Conditional] Data Protection Officer / Privacy Advisor skal gennemgå den privatlivsmæssige konsekvens af væsentlige politikændringer i REG12 før godkendelse.

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

12. Relaterede politikker

12.1 PII01 - Politik for ledelsessystem for databeskyttelsesoplysninger

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

12.3 PII03 - Politik for PII-behandlingsfortegnelse og behandlingsgrundlag

12.4 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.5 PII05 - Politik for styring af samtykke og præferencer

12.6 PII06 - Politik for styring af registreredes rettigheder

12.7 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.8 PII09 - Politik for indsamling, brug, videregivelse og deling af PII

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

12.10 PII11 - Politik for korrekthed og kvalitet af PII

12.11 PII12 - Politik for privatlivsstyring af databehandlere, underdatabehandlere og tredjeparter

12.12 PII13 - Politik for international overførsel af PII

12.13 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.14 PII17 - Politik for PIMS-dokumenteret information og evidensstyring

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

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 6.1.2; Clause 6.1.3** - Kortlagt til screening af databeskyttelsesrisiko, kobling til behandlingshandlinger, analyse af designafhængigheder, eskalering og korrigerende handling uden at duplikere den fulde metode for databeskyttelsesrisiko og DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Kortlagt til planlagte ændringer vedrørende databeskyttelse, projektopstart, operationel gennemgang af databeskyttelse gennem design, idriftsættelseskontrol og gennemgang af væsentlige ændringer. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Kortlagt til dokumentation for databeskyttelse gennem design, der opbevares i REG02, REG04, REG08 og REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Kortlagt til metrikker for databeskyttelse gennem design, stikprøver af dokumentation, registrering af afvigelser, korrigerende handling og verifikation af effektivitet. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Kortlagt til dokumentation af behandlingsformål, behandlingsregistreringer, kobling til databeskyttelse gennem design og udløsere for databeskyttelsesrisiko eller DPIA-screening ved behandling som dataansvarlig. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Kortlagt til begrænsning af indsamling og behandling af PII gennem formålsbaserede minimumsdatakrav, valgfrie behandlinger slået fra som standard og minimale standardindstillinger for behandling. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Kortlagt til dirigering af korrekthedsafhængigheder, minimeringsmål, gennemførlighed af afidentificering og designdokumentation for minimering af identificerbar PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Kortlagt til identifikation i designfasen af afidentificering, sletningsafhængighed, midlertidige PII-artefakter og dirigering til livscykluskontroller uden at duplikere udførelse af opbevaring eller bortskaffelse. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Kortlagt til databehandlerens kundeinstrukser, kundesupportoplysninger, databehandlerens designregistreringer og kundeautoriserede ændringer af tjenestedesign. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Kortlagt til databehandlerens designkapaciteter for midlertidige filer, afhængighed af returnering eller bortskaffelse og afhængighed af transmissionskontrol registreret som designdokumentation uden at duplikere operationelle sletnings- eller sikkerhedskontrolprocedurer. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Kortlagt til krav til databeskyttelse i udviklingslivscyklussen, tekniske principper, kontrolpunkter for PII-beskyttelse og dokumentation for standardkonfiguration for databeskyttelse. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Kortlagt til formålsbegrænsning, minimalt PII-design, kobling til behandlingsregistreringer, standardminimering, dokumentation og

ansvarlighed. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Kortlagt til foranstaltninger hos den dataansvarlige, styringsgennemgang, godkendelse af undtagelser, korrigerende handling og politikvedligeholdelse med henblik på implementering af databeskyttelse gennem design. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Kortlagt til projektopstart, krav til databeskyttelse i designfasen, standardindstillinger for databeskyttelse, minimering, designkontroller ved indkøb, gennemgang før idriftsættelse og ændringsudløst gennemgang. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Kortlagt til databehandlerinstrukser, understøttelse af databehandlerdesign, dokumentation for leverandørers databeskyttelse gennem design og kundeautoriserede designændringer. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Kortlagt til kobling til behandlingsregistreringer, REG02-opdateringer, designafhængigheder for behandlingsaktiviteter og dokumentation for behandlingsregistreringer. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Kortlagt til udløsere for databeskyttelsesrisiko og DPIA-screening i designfasen, højrisikorådgivning og efterimplementeringskontroller uden at duplikere DPIA-metoden. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Kortlagt til identifikation af privatlivskontroller i designfasen, kobling til databeskyttelsesrisiko og designdokumentation for kontrolimplementering. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Kortlagt til formålsspecifikation, begrænsning af indsamling, dataminimering, begrænset brug og standardindstillinger for behandling. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Kortlagt til dirigering af korrekthedsafhængighed, ansvarlighedsdokumentation, overvågning af databeskyttelse gennem design, revision og korrigerende handling. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Kortlagt til formålets legitimitet, begrænsning af indsamling, dataminimering, begrænsning af brug og videregivelse, opbevaringsafhængighed, håndtering af midlertidige filer og designkontroller for korrekthedsafhængighed. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].