					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII07					Dokumenttitel: **Politik for risikovurdering vedrørende databeskyttelse og DPIA**						
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-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 sammenhæng med SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Planlagte PIMS-ændringer og fornyet risikovurdering
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumenterede oplysninger om databeskyttelsesrisiko og DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	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	Supporting	Overvågning og måling af databeskyttelsesrisiko
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Ledelsens gennemgang af databeskyttelsesrisiko
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Risikorelateret afvigelse og korrigerende handling
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Konsekvensanalyse vedrørende privatliv
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Behandlingsregistreringer, der understøtter risikovurdering
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Databehandlers kundeaftale og bistand til DPIA

ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Databehandlers oplysninger til understøttelse af kundens efterlevelse
GDPR	Article 5(2)	Controller	Supporting	Bevismateriale for ansvarlighed
GDPR	Article 24	Controller	Supporting	Dataansvarliges ansvar og foranstaltninger
GDPR	Article 25	Controller	Supporting	Databeskyttelse gennem design og standardindstillinger
GDPR	Article 28	Both	Supporting	Databehandlerbistand og instrukser
GDPR	Article 30	Both	Supporting	Fortegnelser over behandlingsaktiviteter, der understøtter DPIA
GDPR	Article 32	Both	Supporting	Sikkerhedsrisiko og sikkerhedsforanstaltninger
GDPR	Article 35	Controller	Primary	Konsekvensanalyse vedrørende databeskyttelse
GDPR	Article 36	Controller	Primary	Forudgående høring
GDPR	Article 39	Conditional	Supporting	DPO-rådgivning og overvågning, hvor det er relevant
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Kontroller for databeskyttelse, informationssikkerhed og efterlevelse af databeskyttelseskrav
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	PIA-omfang, fordele, udløsende forhold og forberedelse
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Program for beskyttelse af personhenførbare oplysninger (PII) og identifikation af krav
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integration af organisatorisk styring af privatlivsrisici

1. Omfang

1.1 Denne politik fastsætter kravene til risikovurdering vedrørende databeskyttelse, DPIA-screening, gennemførelse af fuld DPIA, risikobehandling, accept af restrisiko, høring, gennemgang og styring af bevismateriale for behandling af personhenførbare oplysninger (PII) inden for PIMS-omfang.

1.2 Denne politik gælder for:

1.2.1 nye og væsentligt ændrede behandlingsaktiviteter vedrørende personhenførbare oplysninger (PII);

1.2.2 behandlingskontekster for dataansvarlig, fælles dataansvarlig, databehandler og underdatabehandler;

1.2.3 systemer, applikationer, tjenester, forretningsprocesser, leverandører, databehandlere, underdatabehandlere, internationale overførsler og datadelingsordninger, der påvirker behandling af personhenførbare oplysninger (PII);

1.2.4 bevismateriale om databeskyttelsesrisiko og DPIA, der vedligeholdes i REG04, samt understøttende bevismateriale, der vedligeholdes i REG02, REG03, REG08, REG09, REG10, REG11 og REG12.

1.3 Denne politik erstatter ikke kontroller for fortegnelse over behandlingsaktiviteter, kontroller for privatlivsmeddelelse, kontroller for samtykke, kontroller for registreredes rettigheder, kontroller for databeskyttelse gennem design, leverandørkontroller, kontroller for internationale overførsler, sikkerhedskontroller for personhenførbare oplysninger (PII), hændelseskontroller, kontroller for dokumenterede oplysninger eller kontroller for overvågning/revision/forbedring. Disse krav er fastsat i de relaterede politikker, der er anført i afsnit 12.

1.4 I denne politik betyder risikovurdering vedrørende databeskyttelse den dokumenterede identifikation, analyse, evaluering, behandling, gennemgang og overvågning af potentielle negative privatlivskonsekvenser, der opstår ved behandling af personhenførbare oplysninger (PII).

1.5 I denne politik betyder DPIA en dokumenteret vurdering, der anvendes ved behandling som dataansvarlig, som sandsynligvis vil medføre høj risiko for registrerede, og som vurderer behandlingens nødvendighed, proportionalitet, risici, sikkerhedsforanstaltninger, restrisiko, behov for høring og godkendelsesbetingelser.

1.6 I denne politik betyder høj restrisiko vedrørende databeskyttelse en databeskyttelsesrisiko, der forbliver over den godkendte accepttærskel efter foreslået eller implementeret risikobehandling.

1.7 I denne politik betyder en væsentlig ændring enhver ændring, der påvirker PIMS-omfang, behandlingsformål, behandlingsgrundlag, kategorier af personhenførbare oplysninger (PII), kategorier af registrerede, behandlingsskala, behandlingsteknologi, overvågning eller profilering, automatiseret beslutningstagning, sårbare registrerede, modtagere, databehandlere, underdatabehandlere, internationale overførsler, opbevaring, sikkerhedskontroller, risikoprofil, kundeinstrukser eller certificeringsomfang.

2. Formål

2.1 Formålet med denne politik er at sikre, at databeskyttelsesrisici og DPIA-forpligtelser identificeres, vurderes, behandles, godkendes, gennemgås og dokumenteres, før behandling af personhenførbare oplysninger (PII) skaber uacceptabel risiko for registrerede eller for PIMS.

2.2 Denne politik gør organisationen i stand til at dokumentere risikobaseret styring af databeskyttelse, ansvarlighed for DPIA som dataansvarlig, bistand til DPIA som databehandler, dokumenteret risikobehandling, godkendelse af restrisiko, beslutningstagning om forudgående høring og løbende forbedring af kontroller for databeskyttelse.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 fastlægge obligatoriske udløsende forhold for screening af databeskyttelsesrisiko;

3.1.2 fastlægge, hvornår en fuld DPIA er påkrævet;

3.1.3 sikre, at DPIA-beslutninger for dataansvarlige dokumenteres og kan gennemgås;

3.1.4 sikre, at bistand til DPIA fra databehandlere og underdatabehandlere dokumenteres, hvor det kræves efter kundeinstruks eller aftale;

3.1.5 sikre, at databeskyttelsesrisici vurderes, før ny eller væsentligt ændret behandling af personhenførbare oplysninger (PII) fortsætter;

3.1.6 sikre, at risikobehandlinger vedrørende databeskyttelse tildeles, implementeres og verificeres;

3.1.7 sikre, at høje restrisici vedrørende databeskyttelse eskaleres og godkendes, før behandling påbegyndes eller fortsættes;

3.1.8 sikre, at beslutninger om forudgående høring dokumenteres, hvor der fortsat er høj restrisiko;

3.1.9 sikre, at bevismateriale om databeskyttelsesrisiko og DPIA vedligeholdes i REG04 og knyttes til relaterede evidensobjekter;

3.1.10 undgå at oprette særskilte DPIA-, risiko- eller høringsregistre uden for REG04.

4. Politikkerklæringer

4.1 Screening af databeskyttelsesrisiko

4.1.1 [Both] Process Owner / Business Owner skal iværksætte screening af databeskyttelsesrisiko i REG04, før ny eller væsentligt ændret behandling af personhenførbare oplysninger (PII), der er registreret i REG02, påbegyndes.

4.1.2 [Both] Privacy Lead / PIMS Manager skal vedligeholde kriterier for screening af databeskyttelsesrisiko i REG04 før den første PIMS-drift og derefter årligt.

4.1.3 [Controller] Process Owner / Business Owner skal gennemføre DPIA-screening i REG04, før behandling som dataansvarlig, der opfylder kriterierne for screening af databeskyttelsesrisiko, påbegyndes.

4.1.4 [Processor] Vendor / Procurement Owner skal registrere kundens krav om bistand til DPIA i REG08, før behandling som databehandler påbegyndes, hvor kundeaftalen eller den dokumenterede instruks kræver DPIA-understøttelse.

4.1.5 [Both] System Owner / Application Owner skal levere bevismateriale om systemdesign, adgang, sikkerhed, logning og dataflows i REG04 før godkendelse af risikovurdering vedrørende databeskyttelse for nye eller væsentligt ændrede systemer, der behandler personhenførbare oplysninger (PII).

4.1.6 [Both] Privacy Lead / PIMS Manager skal registrere screeningsresultatet og begrundelsen for beslutningen om fuld DPIA i REG04, før behandlingsaktiviteten fortsætter.

4.2 Udløsende forhold for DPIA og fastlæggelse af krav

4.2.1 [Controller] Privacy Lead / PIMS Manager skal kræve en fuld DPIA i REG04, før behandling som dataansvarlig, der sandsynligvis vil medføre høj risiko, påbegyndes.

4.2.2 [Controller] Process Owner / Business Owner skal henvise behandling, der omfatter stor skala, systematisk overvågning, profilering, automatiserede afgørelser, særlige kategorier af personoplysninger, oplysninger om straffedomme og lovovertrædelser, sårbare registrerede, innovativ teknologi eller væsentligt ændret behandling, til Privacy Lead / PIMS Manager i REG04, før behandlingen påbegyndes.

4.2.3 [Controller] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG04, før en beslutning om krav om fuld DPIA for behandling som dataansvarlig med høj risiko godkendes.

4.2.4 [Both] Process Owner / Business Owner skal foretage fornyet screening af databeskyttelsesrisiko i REG04, før personhenførbare oplysninger (PII) anvendes til et nyt formål, en ny modtager tilføjes, en ny databehandler eller underdatabehandler introduceres, systemarkitektur ændres, eller en ny international overførsel påbegyndes.

4.2.5 [Processor] Privacy Lead / PIMS Manager skal dokumentere, om understøttelse af DPIA som databehandler er påkrævet i REG08, inden for 10 arbejdsdage efter modtagelse af en kundeanmodning om bistand til DPIA.

4.2.6 [Subprocessor] Vendor / Procurement Owner skal dokumentere krav om bistand til DPIA opstrøms i REG08, før underbehandling påbegyndes, hvor den opstrøms kunde eller databehandleraftale kræver sådan bistand.

[... 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 databeskyttelsesrisiko og DPIA

9.1.1 [All] Process Owner / Business Owner skal anmode om enhver undtagelse fra denne politik i REG12, før afvigelsen finder sted.

9.1.2 [All] Privacy Lead / PIMS Manager skal vurdere den databeskyttelsesmæssige, juridiske, certificeringsmæssige, operationelle og registreredes påvirkning af hver anmodet undtagelse i REG04 eller REG12 inden for 10 arbejdsdage efter anmodningen.

9.1.3 [All] Data Protection Officer / Privacy Advisor skal registrere rådgivning i REG12 før godkendelse af enhver undtagelse, der påvirker behandling med høj risiko, gennemførelse af fuld DPIA, forudgående høring, høj restrisiko vedrørende databeskyttelse eller kundebistand til DPIA.

9.1.4 [All] Top Management skal godkende undtagelser vedrørende databeskyttelsesrisiko eller DPIA, der påvirker behandling med høj risiko, certificeringsomfang, forudgående høring eller uløst høj restrisiko vedrørende databeskyttelse, i REG12, før undtagelsen får virkning.

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

9.1.6 [All] Process Owner / Business Owner skal lukke eller revurdere hver undtagelse vedrørende databeskyttelsesrisiko eller DPIA i REG12 inden for fem arbejdsdage efter udløb.

10. Håndhævelse

10.1 Håndhævelse vedrørende databeskyttelsesrisiko og DPIA

10.1.1 [All] Privacy Lead / PIMS Manager skal registrere manglende, unøjagtigt, ufuldstændigt, forsinket eller ikke-godkendt REG04-bevismateriale vedrørende databeskyttelsesrisiko eller DPIA som en afvigelse i REG12 inden for fem arbejdsdage efter identifikation.

10.1.2 [Controller] Process Owner / Business Owner skal suspendere ny behandling som dataansvarlig med høj risiko, når påkrævet REG04-bevismateriale for DPIA-godkendelse mangler før lancering.

10.1.3 [Both] System Owner / Application Owner skal blokere idriftsættelse af systemer, der behandler personhenførbare oplysninger (PII), når påkrævet REG04-bevismateriale for risikobehandling mangler før godkendelse af idriftsættelse.

10.1.4 [Both] Vendor / Procurement Owner skal blokere onboarding af leverandører, databehandlere, underdatabehandlere eller datadeling, når påkrævet REG04-bevismateriale for databeskyttelsesrisiko eller bistand til DPIA mangler før aftalegodkendelse.

10.1.5 [All] Top Management skal gennemgå uløste større afvigelser vedrørende databeskyttelsesrisiko eller DPIA i REG12 under ledelsens gennemgang.

10.1.6 [All] Privacy Lead / PIMS Manager skal eskalere gentagne overskredne frister for REG04-screening, DPIA-gennemgang eller risikobehandling til Top Management i REG12 inden for fem arbejdsdage efter den anden forekomst i en 12-måneders periode.

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

11. Gennemgang og vedligeholdelse

11.1 Gennemgang og vedligeholdelse af politikken

11.1.1 [All] Privacy Lead / PIMS Manager skal gennemgå denne politik i REG12 årligt og inden for 30 dage efter væsentlig ændring af krav til databeskyttelsesrisiko, DPIA, forudgående høring, databehandlerbistand eller certificering.

11.1.2 [All] Privacy Lead / PIMS Manager skal årligt gennemgå REG04-screeningkriterier, DPIA-udløserkriterier, risikoklassificeringskriterier og kriterier for accept af restrisiko i REG12.

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 opdatere REG03 og REG04 inden for 15 arbejdsdage efter godkendte politikændringer, der ændrer kontrolanvendelighed, risikokriterier eller DPIA-screeningkrav.

11.1.6 [All] Privacy Lead / PIMS Manager skal registrere kommunikation af godkendte ændringer af denne politik 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 roller, ansvar og ansvarlighed vedrørende databeskyttelse

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

12.5 PII04 - Politik for privatlivsmeddelelse og gennemsigtighed

12.6 PII05 - Politik for samtykke- og præferencestyring

12.7 PII06 - Politik for håndtering af registreredes rettigheder

12.8 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

12.9 PII09 - Politik for indsamling, brug, videregivelse og deling af personhenførbare oplysninger (PII)

12.10 PII10 - Politik for opbevaring, sletning og bortskaffelse af personhenførbare oplysninger (PII)

12.11 PII11 - Politik for nøjagtighed og kvalitet af personhenførbare oplysninger (PII)

12.12 PII12 - Politik for databehandler-, underdatabehandler- og tredjepartsstyring vedrørende databeskyttelse

12.13 PII13 - Politik for international overførsel af personhenførbare oplysninger (PII)

12.14 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.15 PII15 - Politik for PII-hændelser og brud

12.16 PII17 - Politik for dokumenterede oplysninger og styring af bevismateriale i PIMS

12.17 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 anførte krav, og identificerer de interne klausuler, der implementerer eller understøtter dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Kortlagt til identifikation og planlægning af handlinger vedrørende databeskyttelsesrisici og -muligheder ved brug af screeningskriterier, risikotærskler, eskalering og input til ledelsens gennemgang. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Kortlagt til gennemførelse af screening af databeskyttelsesrisiko, risikovurdering vedrørende databeskyttelse, risikoklassificering, revurdering og evaluering af udløsende forhold for DPIA, før ny eller væsentligt ændret behandling fortsætter. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Kortlagt til planlægning af risikobehandling vedrørende databeskyttelse, opdateringer af kontrolanvendelighed, implementering af behandling, accept af restrisiko og sammenhæng med SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Kortlagt til planlagte PIMS- og behandlingsændringer, der udløser fornyet risikovurdering vedrørende databeskyttelse og DPIA-gennemgang. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Kortlagt til styrede dokumenterede oplysninger for screening af databeskyttelsesrisiko, DPIA-bevismateriale, risikobehandling, accept af restrisiko, beslutninger om forudgående høring, undtagelser, afvigelser og bevismateriale for gennemgang af politikken. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Kortlagt til drift af kontroller for databeskyttelsesrisiko og DPIA før idriftsættelse, onboarding, behandlingsgodkendelse, lukning af behandling og sammenknytning med korrigerende handlinger. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Kortlagt til operationel risikovurdering vedrørende databeskyttelse for nye og ændrede behandlingsændringer samt system-, leverandør-, overførsels- og hændelsesdrevne behandlingsændringer. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Kortlagt til operationel risikobehandling vedrørende databeskyttelse, tildeling af behandling, implementering af behandling, eskalering af forsinket behandling og verifikation af effektivitet. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Kortlagt til overvågning og måling af screeningsdækning, DPIA-status, åbne risici, forsinkede behandlingshandlinger, leverandørhandlinger, sikkerhedsbehandlingshandlinger, handlinger til revurdering efter hændelser og revisionskonstateringer. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Kortlagt til ledelsens gennemgang af høje restrisici vedrørende databeskyttelse, forsinkede behandlingshandlinger, status for fuld DPIA, beslutninger om

forudgående høring og større undtagelser vedrørende databeskyttelsesrisiko. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Kortlagt til afvigelser vedrørende databeskyttelsesrisiko og DPIA, undtagelser, oprettelse af korrigerende handlinger, eskalering og verifikation af effektivitet. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Kortlagt til vurdering af behovet for, og implementering hvor relevant af, konsekvensanalyse vedrørende privatliv for ny eller ændret behandling som dataansvarlig. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Kortlagt til behandlingsregistreringer, der understøtter input til vurdering af databeskyttelsesrisiko og DPIA, herunder formål, kategorier, systemer, modtagere, overførsler og leverandører. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Kortlagt til databehandlers kundeaftaler og kundens forpligtelser vedrørende bistand til DPIA. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Kortlagt til databehandlers levering af oplysninger, der er nødvendige for kundens efterlevelse, herunder bistand til DPIA og bevismateriale for kundeunderstøttelse. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Kortlagt til bevismateriale for ansvarlighed vedrørende DPIA-screening, beslutninger om fuld DPIA, risikobehandling, accept af restrisiko, beslutninger om forudgående høring, undtagelser, revisionskonstateringer og korrigerende handlinger. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Kortlagt til dataansvarliges ansvar for passende foranstaltninger vedrørende databeskyttelsesrisiko, gennemgang af høj restrisiko, ledelsesgodkendelse og vedligeholdelse af politikken. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Kortlagt til bevismateriale for databeskyttelse gennem design og databeskyttelse som standard, der anvendes i risikovurdering og før godkendelse af idriftsættelse. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Kortlagt til bistand til DPIA fra databehandlere og underdatabehandlere, håndtering af kundeinstrukser og bevismateriale for leverandørrisikobehandling. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Kortlagt til behandlingsregistreringer, der understøtter input til risikovurdering vedrørende databeskyttelse og DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Kortlagt til input om PII-sikkerhedsrisiko, valg af sikkerhedsforanstaltninger, behandling af sikkerhedsrisiko og opdateringer af sikkerhedskontrolstatus. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Kortlagt til DPIA-screening, fastlæggelse af krav om fuld DPIA, DPIA-indhold, DPO-rådgivning, gennemgang og blokering af behandling med høj risiko uden påkrævet DPIA-godkendelse. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Kortlagt til beslutningstagning om forudgående høring, DPO-rådgivning, godkendelse fra Top Management og handlinger vedrørende fortsættelse, suspension, redesign eller høring, hvor der fortsat er høj restrisiko. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Kortlagt til rådgivning og overvågning fra Data Protection Officer / Privacy Advisor, hvor det er relevant for DPIA-beslutninger, behandling med høj risiko, forudgående

høring og politikændringer. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Kortlagt til identifikation af kontroller for databeskyttelse, sikkerhedsforanstaltninger, efterlevelse af databeskyttelseskrav, bevismateriale for databeskyttelsesrisiko, overvågning og gennemgang. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Kortlagt til PIA-processens omfang, fordele, fastlæggelse af udløsende forhold, forberedelse, vurderingsinput, bevismateriale fra interessenter og DPIA-rapportstruktur, der vedligeholdes i REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Kortlagt til krav til program for beskyttelse af personhenførbare oplysninger (PII), identifikation af krav til beskyttelse af personhenførbare oplysninger (PII), risikobaseret kontroludvælgelse og sammenhæng med risikobehandling vedrørende databeskyttelse. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Kortlagt til organisatoriske principper for privatlivsrisiko, lederskab, integration, risikovurdering, risikobehandling, overvågning og gennemgang samt registrering og rapportering. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].