					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: PII23					Dokumenttitel: **Politik for cloudbaseret PII-databehandler**						
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 4.1; Clause 6.1.3	Processor	Supporting	PIMS-rolle og kontrollens anvendelighed
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumenteret bevismateriale for cloudbaseret databehandler og operationel styring
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Overvågning, afvigelser og korrigerende handling
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Kundeaftaler, instrukser, bistand og registreringer
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Kundebistand vedrørende forpligtelser over for registrerede
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Midlertidige filer, returnering, overførsel, bortskaffelse og transmissionskontroller
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Overførselsgrundlag og lokationer
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registreringer af videregivelse og håndtering af anmodninger om videregivelse
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Videregivelse til underdatabehandlere, inddragelse og ændringsmeddelelse
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Bevismateriale for adgang, registreringer, backup og logning
GDPR	Article 28	Processor	Primary	Databehandler, underdatabehandler, bistand, revision, sletning og returnering
GDPR	Article 30	Processor	Supporting	Databehandlerregistreringer
GDPR	Article 32; Article 33	Processor	Supporting	Sikkerhed og underretning om brud til dataansvarlig

GDPR	Article 44	Conditional	Referenced	Routing for internationale overførsler
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Formål, dataminimering, brug, opbevaring og begrænsning af videregivelse
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Ansvarlighed, informationssikkerhed og efterlevelse
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Evaluering og overvågning af databehandler samt ændrings- og opbevaringskontroller
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Kontrollens anvendelighed, operationel styring og leverandør-/cloudkontroller
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Leverandør-, cloud-, sletnings-, lognings- og overvågningskontroller
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Kundebistand og formålsbegrænsning for cloudbaseret databehandler
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Underretning om cloudbaseret videregivelse, registreringer af videregivelse og gennemsigtighed om underleverandører
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Grænseflade for cloudbaserede brud, exit, kontraktlige foranstaltninger, underkontrakter og lokationsregistreringer
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategi og styring for leverandørrelationer
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3;	Processor	Supporting	Planlægning, aftale, styring, overvågning og ophør af leverandørrelationer

	Clause 7.4; Clause 7.5			
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	Processor	Supporting	Ramme og dokumentation for sletning
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	Processor	Supporting	Implementering af sletning og undtagelser

1. Omfang

1.1 Denne politik fastsætter obligatoriske krav til databeskyttelse for cloudtjenester, hvor organisationen fungerer som PII-databehandler eller underdatabehandler, herunder SaaS-, PaaS-, IaaS-, hostede applikations-, administrerede cloud-, cloudsupport-, cloudlagrings-, cloudanalyse- og cloudinfrastrukturtjenester, der behandler PII på vegne af kunder.

1.2 Denne politik gælder for cloudbaseret behandling, der udføres i henhold til kundeaftaler, dokumenterede kundeinstrukser, instrukser fra overordnede databehandlere, underdatabehandlerordninger, konfiguration af cloudregioner, cloudsupportadgang, serviceadministration, backup, replikering, logning, overvågning, sletning, returnering, bistand ved brud, revisionsbistand og forpligtelser til kundebistand.

1.3 Denne politik dækker:

1.3.1 omfang for cloudbaseret PII-behandling og registreringer af instrukser;

1.3.2 bevismateriale for kundeaftaler og delt ansvarsmodel;

1.3.3 bevismateriale for tenant-isolering, cloudadgang, administrativ adgang og logning;

1.3.4 styring af underdatabehandlere og cloudforsyningskæden;

1.3.5 lokation, fjernadgang og routing for internationale overførsler;

1.3.6 bevismateriale for returnering, overførsel, sletning, bortskaffelse og exit;

1.3.7 kundebistand vedrørende registreredes rettigheder, DPIA'er, revisioner og håndtering af brud;

1.3.8 bevismateriale for overvågning, undtagelser, håndhævelse og forbedring.

1.4 Denne politik opretter ikke et særskilt kundekontraktregister, register over cloudtjenester, register over tenant-isolering, adgangsregister, logregister, sletningsregister, supportanmodningsregister, register over revisionsbevismateriale, brudregister, underdatabehandlerregister eller cloudstyringskomité.

1.5 Denne politik erstatter ikke:

1.5.1 PII03 for fortegnelse over behandlingsaktiviteter og ejerskab til behandlingsgrundlag;

1.5.2 PII06 for den fulde arbejdsgang for registreredes rettigheder;

1.5.3 PII07 for metode til risikovurdering vedrørende databeskyttelse og DPIA;

1.5.4 PII08 for kontrolporte for databeskyttelse gennem design og standardindstillinger;

1.5.5 PII09 for generelle kontroller for indsamling, brug, videregivelse og deling;

1.5.6 PII10 for metode til opbevaring, sletning og bortskaffelse;

1.5.7 PII12 for generel livscyklusstyring af databehandlere, underdatabehandlere og tredjeparter;

1.5.8 PII13 for vurdering af mekanismer for internationale overførsler;

1.5.9 PII14 for fuld arkitektur for PII-sikkerhed og adgangsstyring;

1.5.10 PII15 for arbejdsgangen for hændelses- og brudhåndtering;

1.5.11 PII17 for styring af dokumenteret information;

1.5.12 PII18 for PIMS-styring af overvågning, revision og forbedring.

2. Formål

2.1 Formålet med denne politik er at sikre, at cloudbaserede PII-databehandler- og underdatabehandlertjenester drives efter dokumenterede kundeinstrukser, klart behandlingsomfang, kontrollerede underdatabehandlerordninger, passende ansvar for cloudsikkerhed, dokumenteret lokation og routing for overførsler, forpligtelser til kundebistand, bistand ved brud, mulighed for sletning/returnering og revisionsklart bevismateriale.

2.2 Denne politik understøtter revisionsberedskab til certificering efter ISO/IEC 27701:2025 PIMS for cloudbaserede databehandlere og cloudbaserede underdatabehandlere, samtidig med at den forbliver integreret med det eksisterende PIMS-politiksæt og kanoniske bevisobjekter.

3. Mål

3.1 Målene med denne politik er at:

3.1.1 Definere omfanget af cloudbaseret PII-behandling før kunde-onboarding eller væsentlig ændring.

3.1.2 Sikre, at kundeinstrukser registreres, gennemgås og følges.

3.1.3 Vedligeholde bevismateriale for cloudbaserede databehandlere og underdatabehandlere i kanoniske PIMS-registre.

3.1.4 Definere bevismateriale for delt ansvar, tenant-isolering, adgang, logning og lokation uden at duplikere PII-sikkerhedspolitikken.

3.1.5 Kontrollere bevismateriale for onboarding, ændring, videreførelse og overvågning af underdatabehandlere.

3.1.6 Understøtte kunder med registreredes rettigheder, DPIA'er, revisionsanmodninger og håndtering af brud.

3.1.7 Sikre, at bevismateriale for returnering, sletning, overførsel og bortskaffelse opbevares ved exit.

3.1.8 Overvåge kontroller for cloudbaserede databehandlere og drive korrigerende handling ved hjælp af REG12.

4. Politikkerklæringer

4.1 Omfang for cloudbehandling og kundeinstrukser

4.1.1 [Processor] Privacy Lead / PIMS Manager MUST registrere hver cloudbaseret PII-behandlingstjeneste, kundens behandlingsrolle, kilde til kundeinstruks, PII-kategorier, kategorier af registrerede, tjenesteformål, behandlingslokation, afhængighed af underdatabehandler, sletningsafhængighed og overførselsmarkering i REG02 og REG08 før kunde-onboarding eller væsentlig tjenesteændring.

4.1.2 [Processor] Process Owner / Business Owner MUST registrere de dokumenterede kundeinstrukser for cloudbaseret PII-behandling i REG08, før behandlingen påbegyndes.

4.1.3 [Subprocessor] Process Owner / Business Owner MUST registrere instrukser fra overordnet databehandler eller kundegodkendte instrukser i REG08, før PII behandles som cloudbaseret underdatabehandler.

4.1.4 [Processor] Privacy Lead / PIMS Manager MUST registrere anvendeligheden af kontroller for cloudbaseret databehandler i REG03, før en ny cloudbaseret PII-behandlingstjeneste frigives eller ændres væsentligt.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor MUST gennemgå enhver kundeinstruks, der synes uforenelig med dokumenterede kundeforpligtelser, PIMS-krav eller godkendt tjenesteomfang, i REG12, før organisationen handler efter instruksen.

4.1.6 [Processor] Process Owner / Business Owner MUST registrere enhver foreslået behandling af kundens PII uden for dokumenterede kundeinstrukser i REG12 og indhente godkendelse fra Privacy Lead / PIMS Manager, før behandlingen finder sted.

4.2 Cloudkonfiguration, tenant-isolering, adgang og logning

4.2.1 [Processor] Information Security Lead MUST registrere grænsen for det delte ansvar i cloudmiljøet for PII-adgang, administration, logning, backup, kryptering, sårbarhedsstyring og sletning i REG08 før kunde-onboarding eller væsentlig tjenesteændring.

4.2.2 [Processor] System Owner / Application Owner MUST validere kontroller for tenant-isolering eller kundeadskillelse i REG12 før brug i produktionsmiljøet og efter væsentlig arkitekturændring.

4.2.3 [Processor] System Owner / Application Owner MUST kun tildele cloudbaseret administrativ adgang til kundens PII, efter at godkendt forretningsbehov, adgangsomfang, adgangsvarighed og gennemgangsfrekvens er registreret i REG12.

4.2.4 [Processor] Information Security Lead MUST gennemgå privilegeret cloudadgang, supportadgang, adgang til kundens PII og logdækning i REG12 mindst kvartalsvist.

4.2.5 [Processor] System Owner / Application Owner MUST validere adskillelse af produktions-, staging-, test- og supportmiljøer for kundens PII i REG12 før frigivelse og efter væsentlig miljøændring.

4.2.6 [Processor] System Owner / Application Owner MUST registrere lokationer for backup, replikering, loglagring og supportadgang for cloudbaseret kunde-PII i REG02, REG08 eller REG09, før disse lokationer aktiveres eller ændres.

[... 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 [Processor] Process Owner / Business Owner MUST anmode om en undtagelse for cloudbaseret databehandler i REG12 før onboarding, frigivelse, fornyelse eller fortsat brug, når krævet bevismateriale for kundeinstruks, underdatabehandler, lokation, adgang, logning, sletning eller hændelsesgrænseflade er ufuldstændigt.

9.2 [Processor] Data Protection Officer / Privacy Advisor MUST gennemgå anmodninger om undtagelser for cloudbaserede databehandlere med væsentlig betydning for databeskyttelse i REG12 før godkendelse, når undtagelsen påvirker kundeinstrukser, bistand til registrerede, overførsler, underdatabehandlere, sletning, brudbistand eller PII med højt konsekvensniveau.

9.3 [Processor] Top Management MUST godkende højrisiko- eller væsentlige undtagelser for cloudbaserede databehandlere i REG12, før undtagelsen træder i kraft.

9.4 [Processor] Privacy Lead / PIMS Manager MUST tildele en udløbsdato, afhjælpningsansvarlig, gennemgangsdato og note om restrisiko i REG12 for hver godkendt undtagelse for cloudbaseret databehandler før godkendelse.

10. Håndhævelse

10.1 [Processor] Privacy Lead / PIMS Manager MUST blokere kunde-onboarding, tjenestefrigivelse, fornyelse eller fortsat behandling, når krævet bevismateriale i REG02, REG03, REG08, REG09, REG10 eller REG12 mangler, før behandlingen påbegyndes eller fortsættes.

10.2 [Processor] System Owner / Application Owner MUST deaktivere ikke-godkendt cloudadgang, ikke-godkendt regionsbrug, ikke-godkendt replikering, ikke-godkendt supportadgang eller ikke-godkendt dataflow til underdatabehandler inden for én arbejdsdag efter en håndhævelsesbeslutning og registrere færdiggørelse i REG08 eller REG12.

10.3 [Processor] Vendor / Procurement Owner MUST suspendere ny PII-behandling hos en ikke-godkendt eller afvigende cloudbaseret underdatabehandler, indtil bevismateriale for korrigerende handling i REG08 er fuldstændigt.

10.4 [Processor] Incident Response Coordinator MUST eskalere overskredne frister for kundeunderretning om hændelser i REG10 og REG12 inden for én arbejdsdag efter identifikation.

10.5 [Processor] Internal Audit / Compliance Reviewer MUST verificere effektiviteten af korrigerende handlinger for større eller gentagne afvigelser vedrørende cloudbaserede databehandlere i REG12 inden for 60 dage efter lukning af den korrigerende handling.

11. Gennemgang og vedligeholdelse

11.1 [Processor] Privacy Lead / PIMS Manager MUST gennemgå denne politik i REG12 årligt og inden for 30 dage efter en væsentlig ændring af forpligtelser for cloudbaserede databehandlere, cloudarkitektur, styring af underdatabehandlere, kundebistand, sletningsmulighed eller certificeringskrav.

11.2 [Processor] Vendor / Procurement Owner MUST gennemgå registreringer over cloudbaserede underdatabehandlere og afhængigheder af cloudtjenester i REG08 mindst årligt og før fornyelse.

11.3 [Processor] System Owner / Application Owner MUST gennemgå bevismateriale for tenant-isolering, privilegeret adgang, logning, backup, replikering og sletning i REG12 mindst årligt og efter væsentlig arkitekturændring.

11.4 [Processor] Privacy Lead / PIMS Manager MUST gennemgå REG09-registreringer over cloudlokationer og routing for overførsler mindst årligt og inden for 15 arbejdsdage efter en væsentlig ændring af lokation, supportadgang, backup eller underdatabehandler.

11.5 [Processor] Privacy Lead / PIMS Manager MUST opdatere REG03 inden for 15 arbejdsdage efter godkendte politikændringer, der påvirker anvendeligheden af kontroller for cloudbaserede databehandlere.

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

12. Relaterede politikker

12.1 Denne politik understøttes af følgende relaterede politikker:

12.2 PII01 - Politik for Privacy Information Management System

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

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

12.5 PII06 - Politik for håndtering af registreredes rettigheder

12.6 PII07 - Politik for risikovurdering vedrørende databeskyttelse og DPIA

12.7 PII08 - Politik for databeskyttelse gennem design og standardindstillinger

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 PII12 - Politik for databehandlere, underdatabehandlere og tredjeparters databeskyttelsesstyring

12.11 PII13 - Politik for international overførsel af PII

12.12 PII14 - Politik for PII-sikkerhed og adgangsstyring

12.13 PII15 - Politik for PII-hændelses- og brudhåndtering

12.14 PII17 - Politik for PIMS-dokumenteret information og styring af bevismateriale

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

12.16 PII20 - Politik for børns privatliv

12.17 PII21 - Politik for AI og automatiseret beslutningstagning vedrørende databeskyttelse

12.18 PII22 - Politik for databeskyttelse ved markedsføring og cookies

12.19 PII24 - Politik for CCTV og fysisk overvågning vedrørende databeskyttelse

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 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 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. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 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. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].