					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII23					Dokumenttitel: **Policy för personuppgiftsbiträde för PII i molntjänster**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / Regelverk	Klausul / Kontroll / Artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	PIMS-roll och kontrolltillämplighet
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumenterat underlag för personuppgiftsbiträde i molntjänster och operativ styrning
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Övervakning, avvikelse och korrigerande åtgärd
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	Kundavtal, instruktioner, stöd och poster
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Kundstöd för skyldigheter avseende registrerade
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Tillfälliga filer, återlämning, överföring, bortskaffning och överföringskontroller
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Grund för överföring och platser
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Poster över utlämnande och hantering av begäran om utlämnande
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Utlämnande till underbiträde, anlitande och meddelande om ändring
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	Underlag för åtkomst, poster, säkerhetskopiering och loggning
GDPR	Article 28	Processor	Primary	Personuppgiftsbiträde, underbiträde, stöd, revision, radering och återlämning

GDPR	Article 30	Processor	Supporting	Register för personuppgiftsbiträden
GDPR	Article 32; Article 33	Processor	Supporting	Säkerhet och incidentanmälan till personuppgiftsansvarig
GDPR	Article 44	Conditional	Referenced	Routning av internationell överföring
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Ändamål, minimering, användning, bevarande och begränsning av utlämnande
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Ansvarsskyldighet, informationssäkerhet och efterlevnad
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	Utvärdering, övervakning, ändring och bevarandekontroller för personuppgiftsbiträden
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	Kontrolltillämplighet, operativ styrning och leverantörs- och molnkontroller
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	Kontroller för leverantörer, molntjänster, radering, loggning och övervakning
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Kundstöd och ändamålsbegränsning för personuppgiftsbiträden i molntjänster
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Molnrelaterad underrättelse om utlämnande, poster över utlämnande och transparens om underbiträden
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11;	Processor	Primary	Gränssnitt för incidenter i molntjänster, exit,

	Annex A.11.12; Annex A.12.1			avtalsåtgärder, underavtal och platsregister
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategi och styrning för leverantörsrelationer
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planering, avtal, hantering, övervakning och avslut av leverantörsrelationer
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	Ramverk och dokumentation för radering
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	Genomförande av radering och undantag

1. Omfattning

1.1 Denna policy fastställer obligatoriska integritetskrav för molntjänster där organisationen agerar som personuppgiftsbiträde eller underbiträde för PII, inklusive SaaS, PaaS, IaaS, driftade applikationer, hanterade molntjänster, molnsupport, molnlagring, molnanalys och molninfrastrukturtjänster som behandlar PII för kunders räkning.

1.2 Denna policy gäller molnbaserad behandling som utförs enligt kundavtal, dokumenterade kundinstruktioner, instruktioner från uppströms personuppgiftsbiträde, upplägg med underbiträden, konfiguration av molnregioner, åtkomst för molnsupport, tjänsteadministration, säkerhetskopiering, replikering, loggning, övervakning, radering, återlämning, stöd vid personuppgiftsincidenter, revisionsstöd och skyldigheter att bistå kunder.

1.3 Denna policy omfattar:

1.3.1 omfattning för behandling av PII i molntjänster och instruktionsposter;

1.3.2 underlag för kundavtal och delat ansvar;

1.3.3 underlag för tenantisolering, åtkomst till molntjänster, administrativ åtkomst och loggning;

1.3.4 styrning av underbiträden och leveranskedja för molntjänster;

1.3.5 plats, fjärråtkomst och routning för internationell överföring;

1.3.6 underlag för återlämning, överföring, radering, bortskaffning och exit;

1.3.7 kundstöd för registrerades rättigheter, DPIA, revisioner och respons på personuppgiftsincidenter;

1.3.8 underlag för övervakning, undantag, tillämpning och förbättring.

1.4 Denna policy skapar inte ett separat kundavtalsregister, register över molntjänster, register över tenantisolering, åtkomstregister, loggregister, raderingsregister, register över supportförfrågningar, register över revisionsunderlag, incidentregister, register över underbiträden eller någon styrningskommitté för molntjänster.

1.5 Denna policy ersätter inte:

1.5.1 PII03 för behandlingsregister och ägarskap för rättslig grund;

1.5.2 PII06 för fullständigt arbetsflöde avseende registrerades rättigheter;

1.5.3 PII07 för metodik för integritetsrisker och DPIA;

1.5.4 PII08 för integritetsskydd genom design och dataskydd som standard;

1.5.5 PII09 för allmänna kontroller för insamling, användning, utlämnande och delning;

1.5.6 PII10 för metodik för bevarande, radering och bortskaffning;

1.5.7 PII12 för allmän livscykelstyrning av personuppgiftsbiträden, underbiträden och tredje parter;

1.5.8 PII13 för bedömning av mekanismer för internationell överföring;

1.5.9 PII14 för fullständig arkitektur för PII-säkerhet och åtkomstkontroll;

1.5.10 PII15 för arbetsflöde för incident- och personuppgiftsincidenthantering;

1.5.11 PII17 för styrning av dokumenterad information;

1.5.12 PII18 för styrning av PIMS-övervakning, revision och förbättring.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att molntjänster där organisationen är personuppgiftsbiträde eller underbiträde för PII drivs enligt dokumenterade kundinstruktioner, tydlig behandlingsomfattning, kontrollerade upplägg med underbiträden, lämpliga säkerhetsansvar i molntjänster, dokumenterad plats och överföringsroutning, skyldigheter att bistå kunder, stöd vid personuppgiftsincidenter, förmåga till radering/återlämning samt underlag med beredskap för revision.

2.2 Denna policy stödjer beredskap för ISO/IEC 27701:2025 PIMS-certifiering för personuppgiftsbiträden och underbiträden i molntjänster, samtidigt som den är integrerad med den befintliga PIMS-policyuppsättningen och kanoniska underlagsobjekt.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 Definiera omfattningen för behandling av PII i molntjänster före kundintroduktion eller väsentlig ändring.

3.1.2 Säkerställa att kundinstruktioner registreras, granskas och följs.

3.1.3 Upprätthålla underlag för personuppgiftsbiträden och underbiträden i molntjänster i kanoniska PIMS-register.

3.1.4 Definiera underlag för delat ansvar, tenantisolering, åtkomst, loggning och plats utan att duplicera policyn för PII-säkerhet.

3.1.5 Kontrollera underlag för introduktion, ändring, vidareföring och övervakning av underbiträden.

3.1.6 Stödja kunder med registrerades rättigheter, DPIA, revisionsförfrågningar och respons på personuppgiftsincidenter.

3.1.7 Säkerställa att underlag för återlämning, radering, överföring och bortskaffning bevaras vid exit.

3.1.8 Övervaka kontroller för personuppgiftsbiträden i molntjänster och driva korrigerande åtgärder med hjälp av REG12.

4. Policyuttalanden

4.1 Omfattning för behandling i molntjänster och kundinstruktioner

4.1.1 [Processor] Privacy Lead / PIMS Manager ska registrera varje tjänst för behandling av PII i molntjänster, kundens behandlingsroll, källa till kundinstruktion, kategorier av PII, kategorier av registrerade, tjänsteändamål, behandlingsplats, beroende av underbiträde, beroende av radering och överföringsflagga i REG02 och REG08 före kundintroduktion eller väsentlig tjänsteändring.

4.1.2 [Processor] Process Owner / Business Owner ska registrera de dokumenterade kundinstruktionerna för behandling av PII i molntjänster i REG08 innan behandlingen börjar.

4.1.3 [Subprocessor] Process Owner / Business Owner ska registrera instruktioner från uppströms personuppgiftsbiträde eller kundgodkända instruktioner i REG08 innan PII behandlas som underbiträde i molntjänster.

4.1.4 [Processor] Privacy Lead / PIMS Manager ska registrera kontrolltillämplighet för personuppgiftsbiträden i molntjänster i REG03 innan en ny tjänst för behandling av PII i molntjänster lanseras eller ändras väsentligt.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor ska granska varje kundinstruktion som förefaller vara oförenlig med dokumenterade kundskyldigheter, PIMS-krav eller godkänd tjänsteomfattning i REG12 innan organisationen agerar enligt instruktionen.

4.1.6 [Processor] Process Owner / Business Owner ska registrera varje föreslagen behandling av kundens PII utanför dokumenterade kundinstruktioner i REG12 och inhämta godkännande från Privacy Lead / PIMS Manager innan behandlingen sker.

4.2 Molnkonfiguration, tenantisolering, åtkomst och loggning

4.2.1 [Processor] Information Security Lead ska registrera gränsen för delat ansvar i molntjänsten för åtkomst till PII, administration, loggning, säkerhetskopiering, kryptering, hantering av sårbarheter och radering i REG08 före kundintroduktion eller väsentlig tjänsteändring.

4.2.2 [Processor] System Owner / Application Owner ska validera kontroller för tenantisolering eller kundsegregering i REG12 före produktionsanvändning och efter väsentlig arkitekturändring.

4.2.3 [Processor] System Owner / Application Owner ska bevilja administrativ åtkomst i molntjänster till kundens PII endast efter att godkänt verksamhetsbehov, åtkomstomfattning, åtkomsttid och granskningsfrekvens har registrerats i REG12.

4.2.4 [Processor] Information Security Lead ska granska privilegierad åtkomst i molntjänster, supportåtkomst, åtkomst till kundens PII och loggtäckning i REG12 minst kvartalsvis.

4.2.5 [Processor] System Owner / Application Owner ska validera separation mellan produktions-, staging-, test- och supportmiljöer för kundens PII i REG12 före release och efter väsentlig miljöändring.

4.2.6 [Processor] System Owner / Application Owner ska registrera platser för säkerhetskopiering, replikering, logglagring och supportåtkomst för kundens PII i molntjänster i REG02, REG08 eller REG09 innan dessa platser aktiveras eller ändras.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1 [Processor] Process Owner / Business Owner ska begära ett undantag för personuppgiftsbiträde i molntjänster i REG12 före introduktion, release, förnyelse eller fortsatt användning när nödvändigt underlag för kundinstruktion, underbiträde, plats, åtkomst, loggning, radering eller incidentgränssnitt är ofullständigt.

9.2 [Processor] Data Protection Officer / Privacy Advisor ska granska undantagsbegäranden för personuppgiftsbiträden i molntjänster som är betydelsefulla för integritetsskyddet i REG12 före godkännande när undantaget påverkar kundinstruktioner, stöd för registrerade, överföringar, underbiträden, radering, stöd vid personuppgiftsincidenter eller personuppgifter med hög påverkan.

9.3 [Processor] Top Management ska godkänna högriskrelaterade eller väsentliga undantag för personuppgiftsbiträden i molntjänster i REG12 innan undantaget träder i kraft.

9.4 [Processor] Privacy Lead / PIMS Manager ska ange utgångsdatum, åtgärdsansvarig, granskningsdatum och notering om kvarstående risk i REG12 för varje godkänt undantag för personuppgiftsbiträde i molntjänster före godkännande.

10. Tillämpning

10.1 [Processor] Privacy Lead / PIMS Manager ska blockera kundintroduktion, tjänsterelease, förnyelse eller fortsatt behandling när nödvändigt underlag i REG02, REG03, REG08, REG09, REG10 eller REG12 saknas innan behandlingen börjar eller fortsätter.

10.2 [Processor] System Owner / Application Owner ska inaktivera icke godkänd åtkomst i molntjänster, icke godkänd användning av region, icke godkänd replikering, icke godkänd supportåtkomst eller icke godkänt dataflöde till underbiträde inom en arbetsdag efter ett beslut om tillämpning och registrera slutförandet i REG08 eller REG12.

10.3 [Processor] Vendor / Procurement Owner ska avbryta ny behandling av PII hos ett icke godkänt eller avvikande underbiträde i molntjänster tills underlag för korrigerande åtgärd i REG08 är komplett.

10.4 [Processor] Incident Response Coordinator ska eskalera missade tidsfrister för kundunderrättelse om incident i REG10 och REG12 inom en arbetsdag efter identifiering.

10.5 [Processor] Internal Audit / Compliance Reviewer ska verifiera effekten av korrigerande åtgärder för större eller upprepade avvikelser hos personuppgiftsbiträden i molntjänster i REG12 inom 60 dagar efter att den korrigerande åtgärden har stängts.

11. Granskning och underhåll

11.1 [Processor] Privacy Lead / PIMS Manager ska granska denna policy i REG12 årligen och inom 30 dagar efter en väsentlig ändring av skyldigheter för personuppgiftsbiträden i molntjänster, molnarkitektur, styrning av underbiträden, kundstöd, raderingsförmåga eller certifieringskrav.

11.2 [Processor] Vendor / Procurement Owner ska granska poster över underbiträden i molntjänster och beroenden av molntjänster i REG08 minst årligen och före förnyelse.

11.3 [Processor] System Owner / Application Owner ska granska underlag för tenantisolering, privilegierad åtkomst, loggning, säkerhetskopiering, replikering och radering i REG12 minst årligen och efter väsentlig arkitekturändring.

11.4 [Processor] Privacy Lead / PIMS Manager ska granska REG09-poster över molnplatser och överföringsroutning minst årligen och inom 15 arbetsdagar efter en väsentlig ändring av plats, supportåtkomst, säkerhetskopiering eller underbiträde.

11.5 [Processor] Privacy Lead / PIMS Manager ska uppdatera REG03 inom 15 arbetsdagar efter godkända policyändringar som påverkar kontrolltillämplighet för personuppgiftsbiträden i molntjänster.

11.6 [All] Top Management ska godkänna väsentliga revideringar av denna policy i REG12 före publicering.

12. Relaterade policyer

12.1 Denna policy stöds av följande relaterade policyer:

12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.4 PII03 - Policy för behandlingsregister för PII och rättslig grund

12.5 PII06 - Policy för hantering av registrerades rättigheter

12.6 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.7 PII08 - Policy för integritetsskydd genom design och dataskydd som standard

12.8 PII09 - Policy för insamling, användning, utlämnande och delning av PII

12.9 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.10 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.11 PII13 - Policy för internationell överföring av PII

12.12 PII14 - Policy för säkerhet och åtkomstkontroll för PII

12.13 PII15 - Policy för incident- och personuppgiftsincidenthantering för PII

12.14 PII17 - Policy för dokumenterad information och underlag i PIMS

12.15 PII18 - Policy för övervakning, revision och förbättring av PIMS

12.16 PII20 - Policy för barns integritet

12.17 PII21 - Policy för integritet vid AI och automatiserat beslutsfattande

12.18 PII22 - Policy för marknadsföringsintegritet och cookies

12.19 PII24 - Policy för CCTV och fysisk övervakning

13. Referensstandarder och ramverk

13.1 Denna policy är mappad till följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som genomför eller stödjer 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].