					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: PII23					Documenttitel: **Beleid voor cloudverwerkers van persoonlijk identificeerbare informatie (PII)**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm / regelgeving	Clausule / beheersmaatregel / artikel	Toepasselijkheid	Dekkingssoort	Opmerking
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	PIMS-rol en toepasselijkheid van beheersmaatregelen
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Gedocumenteerd bewijsmateriaal voor cloudverwerkers en operationele beheersing
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitoring, non-conformiteit en corrigerende maatregelen
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	Klantovereenkomsten, instructies, ondersteuning en registraties
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Klantondersteuning voor verplichtingen inzake betrokkenen
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Tijdelijke bestanden, teruggave, doorgifte, afvoer en beheersmaatregelen voor transmissie
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Grondslag voor doorgifte en locaties
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registraties van verstrekkingen en afhandeling van verzoeken om verstrekking
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Verstrekking aan subverwerkers, inschakeling en kennisgeving van wijzigingen
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	Bewijsmateriaal voor toegang, registraties, back-up en logging
GDPR	Article 28	Processor	Primary	Verwerker, subverwerker, ondersteuning, audit, verwijdering en teruggave
GDPR	Article 30	Processor	Supporting	Verwerkersregistraties

GDPR	Article 32; Article 33	Processor	Supporting	Beveiliging en melding van inbreuken aan de verwerkingsverantwoordelijke
GDPR	Article 44	Conditional	Referenced	Routing van internationale doorgifte
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Doelbinding, minimalisatie, gebruik, bewaring en beperking van verstrekking
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Verantwoordingsplicht, informatiebeveiliging en naleving
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	Evaluatie en monitoring van verwerkers, wijzigingen en beheersmaatregelen voor bewaring
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	Toepasselijkheid van beheersmaatregelen, operationele beheersing en beheersmaatregelen voor leveranciers/cloud
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	Beheersmaatregelen voor leveranciers, cloud, verwijdering, logging en monitoring
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Klantondersteuning door cloudverwerker en doelbinding
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Cloudkennisgeving van verstrekking, registraties van verstrekkingen en transparantie over subverwerkers
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	Cloudinterface voor inbreuken, exit, contractuele maatregelen, subcontracten en locatieregistraties
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategie en governance voor leveringsrelaties
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3;	Processor	Supporting	Planning, overeenkomst, beheer, monitoring en

	Clause 7.4; Clause 7.5			beëindiging van leveranciersrelaties
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	Kader voor verwijdering en documentatie
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	Implementatie van verwijdering en uitzonderingen

1. Reikwijdte

1.1 Dit beleid definieert verplichte privacyvereisten voor in de cloud gehoste diensten waarbij de organisatie optreedt als verwerker of subverwerker van persoonlijk identificeerbare informatie (PII), waaronder SaaS-, PaaS-, IaaS-, gehoste applicatie-, managed-cloud-, cloudsupport-, cloudopslag-, cloudanalyse- en cloudinfrastructuurdiensten die persoonlijk identificeerbare informatie (PII) namens klanten verwerken.

1.2 Dit beleid is van toepassing op cloudverwerking die wordt uitgevoerd op grond van klantovereenkomsten, gedocumenteerde klantinstructies, instructies van bovenliggende verwerkers, subverwerkersregelingen, configuratie van cloudregio's, toegang voor cloudsupport, servicebeheer, back-up, replicatie, logging, monitoring, verwijdering, teruggave, ondersteuning bij inbreuken, ondersteuning bij audits en verplichtingen tot ondersteuning van klanten.

1.3 Dit beleid omvat:

1.3.1 reikwijdte van cloudverwerking van persoonlijk identificeerbare informatie (PII) en instructieregistraties;

1.3.2 bewijsmateriaal voor klantovereenkomsten en gedeelde verantwoordelijkheid;

1.3.3 bewijsmateriaal voor tenantisolatie, cloudtoegang, beheerderstoegang en logging;

1.3.4 governance van subverwerkers en de cloudtoeleveringsketen;

1.3.5 locatie, toegang op afstand en routing van internationale doorgifte;

1.3.6 bewijsmateriaal voor teruggave, doorgifte, verwijdering, afvoer en exit;

1.3.7 klantondersteuning voor rechten van betrokkenen, DPIA's, audits en respons op inbreuken;

1.3.8 bewijsmateriaal voor monitoring, uitzonderingen, handhaving en verbetering.

1.4 Dit beleid creëert geen afzonderlijk register voor klantcontracten, register van clouddiensten, register voor tenantisolatie, toegangsregister, logregister, verwijderingsregister, register voor supportverzoeken, register voor auditbewijsmateriaal, register voor inbreuken, subverwerkersregister of cloudgovernancecomité.

1.5 Dit beleid vervangt niet:

1.5.1 PII03 voor de verwerkingsinventaris en eigenaarschap van de rechtsgrondslag;

1.5.2 PII06 voor de volledige workflow voor rechten van betrokkenen;

1.5.3 PII07 voor de methodologie voor privacyrisico's en DPIA's;

1.5.4 PII08 voor privacy by design- en privacy-by-default-poorten;

1.5.5 PII09 voor algemene beheersmaatregelen voor verzameling, gebruik, verstrekking en delen;

1.5.6 PII10 voor de methodologie voor bewaring, verwijdering en afvoer;

1.5.7 PII12 voor algemene governance van de levenscyclus van verwerkers, subverwerkers en derde partijen;

1.5.8 PII13 voor beoordeling van mechanismen voor internationale doorgifte;

1.5.9 PII14 voor de volledige beveiligings- en toegangscontrolearchitectuur voor persoonlijk identificeerbare informatie (PII);

1.5.10 PII15 voor de workflow voor incident- en inbreukbeheer;

1.5.11 PII17 voor beheersing van gedocumenteerde informatie;

1.5.12 PII18 voor PIMS-governance inzake monitoring, audit en verbetering.

2. Doel

2.1 Het doel van dit beleid is te waarborgen dat cloud-PII-verwerkersdiensten en cloud-PII-subverwerkersdiensten worden uitgevoerd op basis van gedocumenteerde klantinstructies, een

duidelijke verwerkingsreikwijdte, beheerste subverwerkersregelingen, passende verantwoordelijkheden voor cloudbeveiliging, gedocumenteerde locatie en routing van doorgiften, verplichtingen tot ondersteuning van klanten, ondersteuning bij inbreuken, mogelijkheden voor verwijdering/teruggave en bewijsmateriaal dat geschikt is voor audits.

2.2 Dit beleid ondersteunt de gereedheid voor certificering volgens ISO/IEC 27701:2025 PIMS voor cloudverwerkers en cloudsubverwerkers, terwijl het geïntegreerd blijft met de bestaande PIMS-beleidsset en canonieke bewijsobjecten.

3. Doelstellingen

3.1 De doelstellingen van dit beleid zijn:

3.1.1 De reikwijdte van cloudverwerking van persoonlijk identificeerbare informatie (PII) definiëren vóór klantonboarding of een wezenlijke wijziging.

3.1.2 Waarborgen dat klantinstructies worden geregistreerd, beoordeeld en opgevolgd.

3.1.3 Bewijsmateriaal voor cloudverwerkers en subverwerkers onderhouden in canonieke PIMS-registers.

3.1.4 Bewijsmateriaal definiëren voor gedeelde verantwoordelijkheid, tenantisolatie, toegang, logging en locatie zonder het PII-beveiligingsbeleid te dupliceren.

3.1.5 Bewijsmateriaal voor onboarding, wijzigingen, doorlegverplichtingen en monitoring van subverwerkers beheersen.

3.1.6 Klanten ondersteunen bij rechten van betrokkenen, DPIA's, auditverzoeken en respons op inbreuken.

3.1.7 Waarborgen dat bewijsmateriaal voor teruggave, verwijdering, doorgifte en afvoer bij exit wordt bewaard.

3.1.8 Beheersmaatregelen voor cloudverwerkers monitoren en corrigerende maatregelen aansturen met REG12.

4. Beleidsverklaringen

4.1 Reikwijdte van cloudverwerking en klantinstructies

4.1.1 [Processor] De Privacy Lead / PIMS Manager moet elke cloudverwerkingsdienst voor persoonlijk identificeerbare informatie (PII), klantverwerkingsrol, bron van de klantinstructie, PII-categorieën, categorieën betrokkenen, servicedoel, verwerkingslocatie, subverwerkersafhankelijkheid, verwijderingsafhankelijkheid en doorgiftevlag in REG02 en REG08 registreren vóór klantonboarding of een wezenlijke dienstwijziging.

4.1.2 [Processor] De Process Owner / Business Owner moet de gedocumenteerde klantinstructies voor cloudverwerking van persoonlijk identificeerbare informatie (PII) in REG08 registreren voordat de verwerking begint.

4.1.3 [Subprocessor] De Process Owner / Business Owner moet instructies van de bovenliggende verwerker of door de klant goedgekeurde instructies in REG08 registreren voordat persoonlijk identificeerbare informatie (PII) als cloudsubverwerker wordt verwerkt.

4.1.4 [Processor] De Privacy Lead / PIMS Manager moet de toepasselijkheid van beheersmaatregelen voor cloudverwerkers in REG03 registreren voordat een nieuwe cloudverwerkingsdienst voor persoonlijk identificeerbare informatie (PII) wordt vrijgegeven of wezenlijk wordt gewijzigd.

4.1.5 [Processor] De Data Protection Officer / Privacy Advisor moet elke klantinstructie die strijdig lijkt met gedocumenteerde klantverplichtingen, PIMS-vereisten of de goedgekeurde servicereikwijdte in REG12 beoordelen voordat de organisatie naar de instructie handelt.

4.1.6 [Processor] De Process Owner / Business Owner moet elke voorgestelde verwerking van klant-PII buiten gedocumenteerde klantinstructies in REG12 registreren en goedkeuring van de Privacy Lead / PIMS Manager verkrijgen voordat de verwerking plaatsvindt.

4.2 Cloudconfiguratie, tenantisolatie, toegang en logging

4.2.1 [Processor] De Information Security Lead moet de grens van gedeelde verantwoordelijkheid in de cloud voor PII-toegang, beheer, logging, back-up, encryptie, kwetsbaarhedenbeheer en verwijdering in REG08 registreren vóór klantonboarding of een wezenlijke dienstwijziging.

4.2.2 [Processor] De System Owner / Application Owner moet tenantisolatie of beheersmaatregelen voor klantscheiding in REG12 valideren vóór productiegebruik en na een wezenlijke architectuurwijziging.

4.2.3 [Processor] De System Owner / Application Owner moet cloudbeheerderstoegang tot klant-PII alleen verlenen nadat goedgekeurde zakelijke behoefte, toegangsreikwijdte, toegangsduur en beoordelingsfrequentie in REG12 zijn geregistreerd.

4.2.4 [Processor] De Information Security Lead moet geprivilegieerde cloudtoegang, supporttoegang, toegang tot klant-PII en dekking van logboeken ten minste per kwartaal in REG12 beoordelen.

4.2.5 [Processor] De System Owner / Application Owner moet de scheiding van productie-, staging-, test- en supportomgevingen voor klant-PII in REG12 valideren vóór vrijgave en na een wezenlijke omgevingswijziging.

4.2.6 [Processor] De System Owner / Application Owner moet back-up-, replicatie-, logopslag- en supporttoegangslocaties voor klant-PII in de cloud in REG02, REG08 of REG09 registreren voordat deze locaties worden ingeschakeld of gewijzigd.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Uitzonderingen

9.1 [Processor] De Process Owner / Business Owner moet een uitzondering voor cloudverwerkers in REG12 aanvragen vóór onboarding, vrijgave, verlenging of voortgezet gebruik wanneer vereist bewijsmateriaal voor klantinstructies, subverwerkers, locatie, toegang, logging, verwijdering of incidentinterface onvolledig is.

9.2 [Processor] De Data Protection Officer / Privacy Advisor moet privacy-significante uitzonderingsverzoeken voor cloudverwerkers in REG12 beoordelen vóór goedkeuring wanneer de uitzondering gevolgen heeft voor klantinstructies, ondersteuning van betrokkenen, doorgiften, subverwerkers, verwijdering, ondersteuning bij inbreuken of PII met hoge impact.

9.3 [Processor] Top Management moet hoogrisico- of wezenlijke uitzonderingen voor cloudverwerkers in REG12 goedkeuren voordat de uitzondering van kracht wordt.

9.4 [Processor] De Privacy Lead / PIMS Manager moet voor elke goedgekeurde uitzondering voor cloudverwerkers vóór goedkeuring een vervaldatum, eigenaar van herstelmaatregelen, beoordelingsdatum en restrisiconotitie in REG12 toewijzen.

10. Handhaving

10.1 [Processor] De Privacy Lead / PIMS Manager moet klantonboarding, servicevrijgave, verlenging of voortgezette verwerking blokkeren wanneer vereist bewijsmateriaal in REG02, REG03, REG08, REG09, REG10 of REG12 ontbreekt voordat de verwerking begint of wordt voortgezet.

10.2 [Processor] De System Owner / Application Owner moet niet-goedgekeurde cloudtoegang, niet-goedgekeurd regiogebruik, niet-goedgekeurde replicatie, niet-goedgekeurde supporttoegang

of niet-goedgekeurde gegevensstroom naar subverwerkers binnen één werkdag na een handhavingsbesluit uitschakelen en voltooiing in REG08 of REG12 registreren.

10.3 [Processor] De Vendor / Procurement Owner moet nieuwe PII-verwerking door een niet-goedgekeurde of niet-conforme cloudsubverwerker opschorten totdat bewijsmateriaal voor corrigerende maatregelen in REG08 volledig is.

10.4 [Processor] De Incident Response Coordinator moet gemiste termijnen voor klantmeldingen van incidenten binnen één werkdag na identificatie in REG10 en REG12 escaleren.

10.5 [Processor] De Internal Audit / Compliance Reviewer moet de doeltreffendheid van corrigerende maatregelen voor majeure of herhaalde non-conformiteiten van cloudverwerkers binnen 60 dagen na afsluiting van de corrigerende maatregel in REG12 verifiëren.

11. Beoordeling en onderhoud

11.1 [Processor] De Privacy Lead / PIMS Manager moet dit beleid jaarlijks en binnen 30 dagen na een wezenlijke wijziging in cloudverwerkersverplichtingen, cloudarchitectuur, subverwerkersgovernance, klantondersteuning, verwijderingsmogelijkheid of certificeringsvereisten in REG12 beoordelen.

11.2 [Processor] De Vendor / Procurement Owner moet registraties van cloudsubverwerkers en afhankelijkheden van clouddiensten in REG08 ten minste jaarlijks en vóór verlenging beoordelen.

11.3 [Processor] De System Owner / Application Owner moet bewijsmateriaal voor tenantisolatie, geprivilegieerde toegang, logging, back-up, replicatie en verwijdering in REG12 ten minste jaarlijks en na een wezenlijke architectuurwijziging beoordelen.

11.4 [Processor] De Privacy Lead / PIMS Manager moet REG09-registraties voor cloudlocaties en routing van doorgiften ten minste jaarlijks en binnen 15 werkdagen na een wezenlijke wijziging van locatie, supporttoegang, back-up of subverwerker beoordelen.

11.5 [Processor] De Privacy Lead / PIMS Manager moet REG03 binnen 15 werkdagen bijwerken na goedgekeurde beleidswijzigingen die de toepasselijkheid van beheersmaatregelen voor cloudverwerkers beïnvloeden.

11.6 [All] Top Management moet wezenlijke herzieningen van dit beleid vóór publicatie in REG12 goedkeuren.

12. Gerelateerde beleidslijnen

12.1 Dit beleid wordt ondersteund door de volgende gerelateerde beleidslijnen:

12.2 PII01 - Beleid inzake het privacy-informatiemanagementsysteem

12.3 PII02 - Beleid inzake privacyrollen, verantwoordelijkheden en verantwoordingsplicht

12.4 PII03 - Beleid inzake PII-verwerkingsinventaris en rechtsgrondslag

12.5 PII06 - Beleid inzake beheer van rechten van betrokkenen

12.6 PII07 - Beleid inzake privacyrisicobeoordeling en DPIA

12.7 PII08 - Beleid inzake privacy by design en privacy by default

12.8 PII09 - Beleid inzake verzameling, gebruik, verstrekking en delen van PII

12.9 PII10 - Beleid inzake bewaring, verwijdering en afvoer van PII

12.10 PII12 - Beleid inzake privacymanagement voor verwerkers, subverwerkers en derde partijen

12.11 PII13 - Beleid inzake internationale doorgifte van persoonsgegevens

12.12 PII14 - Beleid inzake beveiliging en toegangscontrole van PII

12.13 PII15 - Beleid inzake incident- en inbreukbeheer voor PII

12.14 PII17 - Beleid inzake gedocumenteerde informatie en bewijsmateriaal in PIMS

12.15 PII18 - Beleid inzake PIMS-monitoring, audit en verbetering

12.16 PII20 - Privacybeleid voor kinderen

12.17 PII21 - Privacybeleid inzake AI en geautomatiseerde besluitvorming

12.18 PII22 - Privacybeleid inzake marketing en cookies

12.19 PII24 - Privacybeleid inzake CCTV en fysieke monitoring

13. Referentienormen en -raamwerken

13.1 Dit beleid is gekoppeld aan de volgende normen en regelgeving. De mapping legt uit hoe het beleid de aangehaalde vereisten ondersteunt en identificeert de interne clausules die deze implementeren of ondersteunen.

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].