					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII23					Titolo del documento: **Politica per il responsabile del trattamento di PII in cloud**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Ruolo PIMS e applicabilità dei controlli
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Evidenze documentate del responsabile del trattamento in cloud e controllo operativo
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Monitoraggio, non conformità e azione correttiva
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	Accordi con i clienti, istruzioni, supporto e registrazioni
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Assistenza al cliente per gli obblighi relativi agli interessati
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	File temporanei, restituzione, trasferimento, smaltimento e controlli di trasmissione
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Base e localizzazioni dei trasferimenti
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registrazioni delle comunicazioni e gestione delle richieste di comunicazione
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Comunicazione relativa ai sub-responsabili, incarico e avviso di modifica
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	Evidenze relative ad accessi, registrazioni, backup e logging
GDPR	Article 28	Processor	Primary	Responsabile del trattamento, sub-responsabile, assistenza, audit,

				cancellazione e restituzione
GDPR	Article 30	Processor	Supporting	Registrazioni del responsabile del trattamento
GDPR	Article 32; Article 33	Processor	Supporting	Sicurezza e notifica della violazione al titolare del trattamento
GDPR	Article 44	Conditional	Referenced	Instradamento dei trasferimenti internazionali
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Finalità, minimizzazione, uso, conservazione e limitazione della comunicazione
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Responsabilizzazione, sicurezza delle informazioni e conformità
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	Valutazione e monitoraggio del responsabile del trattamento, modifiche e controlli di conservazione
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	Applicabilità dei controlli, controllo operativo e controlli su fornitori/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	Controlli su fornitori, cloud, cancellazione, logging e monitoraggio
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Assistenza al cliente del responsabile del trattamento in cloud e limitazione delle finalità
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Notifica delle comunicazioni in cloud, registrazioni delle comunicazioni e

				trasparenza sui sub-responsabili
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	Interfaccia cloud per le violazioni, uscita, misure contrattuali, subcontratti e registrazioni delle localizzazioni
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategia e governance del rapporto di fornitura
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Pianificazione, accordo, gestione, monitoraggio e cessazione del rapporto con il fornitore
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	Quadro di riferimento e documentazione per la cancellazione
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	Applicazione della cancellazione ed eccezioni

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti obbligatori di privacy per i servizi cloud in cui l'organizzazione agisce come responsabile del trattamento o sub-responsabile di PII, inclusi servizi SaaS, PaaS, IaaS, applicazioni ospitate, cloud gestito, supporto cloud, archiviazione cloud, analisi cloud e servizi di infrastruttura cloud che trattano PII per conto dei clienti.

1.2 La presente politica si applica al trattamento in cloud svolto in base ad accordi con i clienti, istruzioni documentate del cliente, istruzioni del responsabile del trattamento a monte, accordi con sub-responsabili, configurazione delle regioni cloud, accesso per il supporto cloud, amministrazione del servizio, backup, replica, logging, monitoraggio, cancellazione, restituzione, supporto in caso di violazione, supporto all'audit e obblighi di assistenza al cliente.

1.3 La presente politica copre:

1.3.1 l'ambito del trattamento di PII in cloud e le registrazioni delle istruzioni;

1.3.2 le evidenze relative agli accordi con i clienti e alla responsabilità condivisa;

1.3.3 le evidenze relative a isolamento dei tenant, accesso cloud, accessi amministrativi e logging;

1.3.4 la governance dei sub-responsabili e della catena di fornitura cloud;

1.3.5 la localizzazione, l'accesso remoto e l'instradamento dei trasferimenti internazionali;

1.3.6 le evidenze relative a restituzione, trasferimento, cancellazione, smaltimento e uscita;

1.3.7 l'assistenza al cliente per i diritti degli interessati, le DPIA, gli audit e la risposta alle violazioni;

1.3.8 le evidenze relative a monitoraggio, eccezioni, applicazione e miglioramento.

1.4 La presente politica non crea un registro separato dei contratti con i clienti, un registro dei servizi cloud, un registro dell'isolamento dei tenant, un registro degli accessi, un registro dei log, un registro delle cancellazioni, un registro delle richieste di supporto, un registro delle evidenze di audit, un registro delle violazioni, un registro dei sub-responsabili o un comitato di governance cloud.

1.5 La presente politica non sostituisce:

1.5.1 PII03 per l'inventario dei trattamenti e la titolarità della base giuridica;

1.5.2 PII06 per il flusso di lavoro completo relativo ai diritti degli interessati;

1.5.3 PII07 per la metodologia di valutazione del rischio privacy e DPIA;

1.5.4 PII08 per i gate di privacy by design e privacy by default;

1.5.5 PII09 per i controlli generali su raccolta, uso, comunicazione e condivisione;

1.5.6 PII10 per la metodologia di conservazione, cancellazione e smaltimento;

1.5.7 PII12 per la governance generale del ciclo di vita di responsabili del trattamento, sub-responsabili e terze parti;

1.5.8 PII13 per la valutazione degli strumenti di trasferimento internazionale;

1.5.9 PII14 per l'architettura completa di sicurezza della PII e controllo degli accessi;

1.5.10 PII15 per il flusso di lavoro di gestione degli incidenti e delle violazioni;

1.5.11 PII17 per il controllo delle informazioni documentate;

1.5.12 PII18 per la governance del monitoraggio, dell'audit e del miglioramento del PIMS.

2. Finalità

2.1 La finalità della presente politica è assicurare che i servizi cloud in qualità di responsabile del trattamento e sub-responsabile di PII operino in base a istruzioni documentate del cliente, ambito del trattamento chiaro, accordi controllati con sub-responsabili, adeguate responsabilità di sicurezza cloud, localizzazione e instradamento dei trasferimenti documentati, obblighi di

assistenza al cliente, supporto in caso di violazione, capacità di cancellazione/restituzione ed evidenze disponibili in sede di audit.

2.2 La presente politica supporta la preparazione alla certificazione PIMS ISO/IEC 27701:2025 per responsabili del trattamento cloud e sub-responsabili cloud, restando integrata con l'insieme esistente di politiche PIMS e con gli elementi di evidenza canonici.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 Definire l'ambito del trattamento di PII in cloud prima dell'onboarding del cliente o di una modifica sostanziale.

3.1.2 Assicurare che le istruzioni del cliente siano registrate, riesaminate e seguite.

3.1.3 Mantenere le evidenze relative al responsabile del trattamento cloud e ai sub-responsabili nei registri PIMS canonici.

3.1.4 Definire le evidenze relative a responsabilità condivisa, isolamento dei tenant, accesso, logging e localizzazione senza duplicare la politica di sicurezza della PII.

3.1.5 Controllare le evidenze relative a onboarding, modifiche, obblighi a cascata e monitoraggio dei sub-responsabili.

3.1.6 Supportare i clienti in relazione ai diritti degli interessati, alle DPIA, alle richieste di audit e alla risposta alle violazioni.

3.1.7 Assicurare che le evidenze relative a restituzione, cancellazione, trasferimento e smaltimento siano conservate all'uscita.

3.1.8 Monitorare i controlli del responsabile del trattamento cloud e promuovere azioni correttive tramite REG12.

4. Dichiarazioni della politica

4.1 Ambito del trattamento in cloud e istruzioni del cliente

4.1.1 [Processor] Privacy Lead / PIMS Manager DEVE registrare ciascun servizio di trattamento di PII in cloud, il ruolo di trattamento del cliente, la fonte delle istruzioni del cliente, le categorie di PII, le categorie di interessati, la finalità del servizio, la localizzazione del trattamento, la dipendenza da sub-responsabili, la dipendenza per la cancellazione e l'indicatore di trasferimento in REG02 e REG08 prima dell'onboarding del cliente o di una modifica sostanziale del servizio.

4.1.2 [Processor] Process Owner / Business Owner DEVE registrare in REG08 le istruzioni documentate del cliente per il trattamento di PII in cloud prima dell'inizio del trattamento.

4.1.3 [Subprocessor] Process Owner / Business Owner DEVE registrare in REG08 le istruzioni del responsabile del trattamento a monte o approvate dal cliente prima di trattare PII in qualità di sub-responsabile cloud.

4.1.4 [Processor] Privacy Lead / PIMS Manager DEVE registrare in REG03 l'applicabilità dei controlli del responsabile del trattamento cloud prima del rilascio o della modifica sostanziale di un nuovo servizio di trattamento di PII in cloud.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor DEVE riesaminare in REG12 qualsiasi istruzione del cliente che appaia non coerente con gli obblighi documentati del cliente, i requisiti PIMS o l'ambito del servizio approvato prima che l'organizzazione dia seguito all'istruzione.

4.1.6 [Processor] Process Owner / Business Owner DEVE registrare in REG12 qualsiasi trattamento proposto di PII del cliente al di fuori delle istruzioni documentate del cliente e ottenere l'approvazione di Privacy Lead / PIMS Manager prima che il trattamento abbia luogo.

4.2 Configurazione cloud, isolamento dei tenant, accesso e logging

4.2.1 [Processor] Information Security Lead DEVE registrare in REG08 il confine della responsabilità condivisa nel cloud per accesso alla PII, amministrazione, logging, backup, cifratura, gestione delle vulnerabilità e cancellazione prima dell'onboarding del cliente o di una modifica sostanziale del servizio.

4.2.2 [Processor] System Owner / Application Owner DEVE validare in REG12 i controlli di isolamento dei tenant o di segregazione dei clienti prima dell'uso in produzione e dopo una modifica sostanziale dell'architettura.

4.2.3 [Processor] System Owner / Application Owner DEVE concedere accessi amministrativi cloud alla PII del cliente solo dopo che l'esigenza aziendale approvata, l'ambito dell'accesso, la durata dell'accesso e la frequenza di riesame sono stati registrati in REG12.

4.2.4 [Processor] Information Security Lead DEVE riesaminare in REG12 gli accessi cloud privilegiati, l'accesso per il supporto, l'accesso alla PII del cliente e la copertura dei log almeno trimestralmente.

4.2.5 [Processor] System Owner / Application Owner DEVE validare in REG12 la separazione degli ambienti di produzione, staging, test e supporto per la PII del cliente prima del rilascio e dopo una modifica sostanziale dell'ambiente.

4.2.6 [Processor] System Owner / Application Owner DEVE registrare le localizzazioni di backup, replica, archiviazione dei log e accesso per il supporto per la PII del cliente in cloud in REG02, REG08 o REG09 prima di abilitare o modificare tali localizzazioni.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Eccezioni

9.1 [Processor] Process Owner / Business Owner DEVE richiedere in REG12 un'eccezione relativa al responsabile del trattamento cloud prima di onboarding, rilascio, rinnovo o uso continuativo quando le evidenze richieste relative a istruzioni del cliente, sub-responsabili, localizzazione, accesso, logging, cancellazione o interfaccia per gli incidenti sono incomplete.

9.2 [Processor] Data Protection Officer / Privacy Advisor DEVE riesaminare in REG12 le richieste di eccezione del responsabile del trattamento cloud rilevanti per la privacy prima dell'approvazione quando l'eccezione incide su istruzioni del cliente, assistenza agli interessati, trasferimenti, sub-responsabili, cancellazione, supporto in caso di violazione o PII ad alto impatto.

9.3 [Processor] Top Management DEVE approvare in REG12 le eccezioni ad alto rischio o sostanziali relative al responsabile del trattamento cloud prima che l'eccezione diventi efficace.

9.4 [Processor] Privacy Lead / PIMS Manager DEVE assegnare in REG12 una data di scadenza, un responsabile della remediation, una data di riesame e una nota sul rischio residuo per ogni eccezione approvata relativa al responsabile del trattamento cloud prima dell'approvazione.

10. Applicazione della politica

10.1 [Processor] Privacy Lead / PIMS Manager DEVE bloccare l'onboarding del cliente, il rilascio del servizio, il rinnovo o il trattamento continuativo quando le evidenze richieste in REG02, REG03, REG08, REG09, REG10 o REG12 sono mancanti prima dell'avvio o della prosecuzione del trattamento.

10.2 [Processor] System Owner / Application Owner DEVE disabilitare l'accesso cloud non approvato, l'uso non approvato di regioni, la replica non approvata, l'accesso per il supporto non approvato o il flusso di dati verso sub-responsabili non approvato entro un giorno lavorativo da una decisione di applicazione della politica e registrare il completamento in REG08 o REG12.

10.3 [Processor] Vendor / Procurement Owner DEVE sospendere il nuovo trattamento di PII da parte di un sub-responsabile cloud non approvato o non conforme finché le evidenze di azione correttiva in REG08 non sono complete.

10.4 [Processor] Incident Response Coordinator DEVE effettuare l'escalation in REG10 e REG12 delle scadenze mancate per la notifica degli incidenti al cliente entro un giorno lavorativo dall'identificazione.

10.5 [Processor] Internal Audit / Compliance Reviewer DEVE verificare in REG12 l'efficacia delle azioni correttive per non conformità maggiori o ripetute relative al responsabile del trattamento cloud entro 60 giorni dalla chiusura dell'azione correttiva.

11. Riesame e manutenzione

11.1 [Processor] Privacy Lead / PIMS Manager DEVE riesaminare la presente politica in REG12 annualmente ed entro 30 giorni da una modifica sostanziale agli obblighi del responsabile del trattamento cloud, all'architettura cloud, alla governance dei sub-responsabili, all'assistenza al cliente, alla capacità di cancellazione o ai requisiti di certificazione.

11.2 [Processor] Vendor / Procurement Owner DEVE riesaminare in REG08 le registrazioni dei sub-responsabili cloud e delle dipendenze da servizi cloud almeno annualmente e prima del rinnovo.

11.3 [Processor] System Owner / Application Owner DEVE riesaminare in REG12 le evidenze relative a isolamento dei tenant, accessi privilegiati, logging, backup, replica e cancellazione almeno annualmente e dopo modifiche sostanziali dell'architettura.

11.4 [Processor] Privacy Lead / PIMS Manager DEVE riesaminare le registrazioni REG09 relative a localizzazioni cloud e instradamento dei trasferimenti almeno annualmente ed entro 15 giorni lavorativi da una modifica sostanziale di localizzazione, accesso per il supporto, backup o sub-responsabile.

11.5 [Processor] Privacy Lead / PIMS Manager DEVE aggiornare REG03 entro 15 giorni lavorativi dalle modifiche approvate alla politica che incidono sull'applicabilità dei controlli del responsabile del trattamento cloud.

11.6 [All] Top Management DEVE approvare le revisioni sostanziali della presente politica in REG12 prima della pubblicazione.

12. Politiche correlate

12.1 La presente politica è supportata dalle seguenti politiche correlate:

12.2 PII01 - Politica del Sistema di gestione delle informazioni sulla privacy

12.3 PII02 - Politica sui ruoli, le responsabilità e la responsabilizzazione in materia di privacy

12.4 PII03 - Politica sull'inventario dei trattamenti di PII e sulla base giuridica

12.5 PII06 - Politica di gestione dei diritti degli interessati

12.6 PII07 - Politica di valutazione del rischio privacy e DPIA

12.7 PII08 - Politica di privacy by design e privacy by default

12.8 PII09 - Politica di raccolta, uso, comunicazione e condivisione della PII

12.9 PII10 - Politica di conservazione, cancellazione e smaltimento della PII

12.10 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.11 PII13 - Politica sui trasferimenti internazionali di PII

12.12 PII14 - Politica di sicurezza della PII e controllo degli accessi

12.13 PII15 - Politica di gestione degli incidenti e delle violazioni di PII

12.14 PII17 - Politica di gestione delle informazioni documentate e delle evidenze PIMS

12.15 PII18 - Politica di monitoraggio, audit e miglioramento del PIMS

12.16 PII20 - Politica sulla privacy dei minori

12.17 PII21 - Politica privacy sull'AI e sul processo decisionale automatizzato

12.18 PII22 - Politica privacy per marketing e cookie

12.19 PII24 - Politica privacy su CCTV e monitoraggio fisico

13. Standard e quadri di riferimento

13.1 La presente politica è mappata ai seguenti standard e normative. La mappatura spiega in che modo la politica supporta i requisiti citati e identifica le clausole interne che li attuano o li supportano.

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].