					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII23					Titre du document : **Politique relative au sous-traitant de PII dans le cloud**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme / Réglementation	Clause / Contrôle / Article	Applicabilité	Type de couverture	Commentaire
ISO/IEC 27701:2025	Clause 4.1; Clause 6.1.3	Processor	Supporting	Rôle PIMS et applicabilité des contrôles
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Éléments de preuve documentés relatifs au sous-traitant cloud et maîtrise opérationnelle
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Surveillance, non-conformité et action corrective
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	Accords clients, instructions, assistance et enregistrements
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Assistance au client pour les obligations relatives aux personnes concernées
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Fichiers temporaires, restitution, transfert, élimination et contrôles de transmission
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Base des transferts et emplacements
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Enregistrements de divulgation et traitement des demandes de divulgation
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Divulgation relative aux sous-traitants ultérieurs, engagement et notification des changements

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	Accès, enregistrements, sauvegarde et éléments de preuve de journalisation
GDPR	Article 28	Processor	Primary	Sous-traitant, sous-traitant ultérieur, assistance, audit, suppression et restitution
GDPR	Article 30	Processor	Supporting	Registres du sous-traitant
GDPR	Article 32; Article 33	Processor	Supporting	Sécurité et notification de violation au responsable du traitement
GDPR	Article 44	Conditional	Referenced	Routage des transferts internationaux
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Limitation de la finalité, minimisation, utilisation, conservation et limitation de la divulgation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Responsabilité, sécurité de l'information et conformité
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	Évaluation, surveillance, changement et contrôles de conservation du sous-traitant
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	Applicabilité des contrôles, maîtrise opérationnelle et contrôles fournisseurs/cloud
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23;	Processor	Supporting	Contrôles fournisseurs, cloud, suppression, journalisation et surveillance

	Control 8.10; Control 8.15; Control 8.16			
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Assistance au client du sous-traitant cloud et limitation de la finalité
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Notification des divulgations cloud, enregistrements de divulgation et transparence des sous-traitants ultérieurs
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	Interface cloud de violation, sortie, mesures contractuelles, sous-contrats et enregistrements des emplacements
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Stratégie et gouvernance de la relation fournisseur
ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planification, accord, gestion, surveillance et résiliation de la relation fournisseur
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	Cadre de suppression et documentation
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	Mise en œuvre de la suppression et exceptions

1. Champ d’application

1.1 La présente politique définit les exigences obligatoires de protection de la vie privée applicables aux services cloud pour lesquels l’organisation agit en qualité de sous-traitant ou de sous-traitant ultérieur de PII, y compris les services SaaS, PaaS, IaaS, les applications hébergées, le cloud managé, le support cloud, le stockage cloud, l’analytique cloud et les services d’infrastructure cloud qui traitent des PII pour le compte de clients.

1.2 La présente politique s’applique aux traitements cloud réalisés en vertu d’accords clients, d’instructions documentées du client, d’instructions d’un sous-traitant amont, d’accords de sous-traitance ultérieure, de la configuration des régions cloud, de l’accès au support cloud, de l’administration des services, de la sauvegarde, de la réplication, de la journalisation, de la surveillance, de la suppression, de la restitution, du support en cas de violation, du support d’audit et des obligations d’assistance au client.

1.3 La présente politique couvre :

1.3.1 le champ du traitement cloud de PII et les enregistrements d’instructions ;

1.3.2 les éléments de preuve relatifs aux accords clients et à la responsabilité partagée ;

1.3.3 les éléments de preuve relatifs à l’isolement des locataires, aux accès cloud, aux accès administratifs et à la journalisation ;

1.3.4 la gouvernance des sous-traitants ultérieurs et de la chaîne d’approvisionnement cloud ;

1.3.5 les emplacements, l’accès à distance et le routage des transferts internationaux ;

1.3.6 les éléments de preuve relatifs à la restitution, au transfert, à la suppression, à l’élimination et à la sortie ;

1.3.7 l’assistance au client pour les droits des personnes concernées, les DPIA, les audits et la réponse aux violations ;

1.3.8 les éléments de preuve relatifs à la surveillance, aux exceptions, à la mise en application et à l’amélioration.

1.4 La présente politique ne crée pas de registre distinct des contrats clients, de registre des services cloud, de registre d’isolement des locataires, de registre des accès, de registre des journaux, de registre des suppressions, de registre des demandes de support, de registre des éléments de preuve d’audit, de registre des violations, de registre des sous-traitants ultérieurs ni de comité de gouvernance cloud.

1.5 La présente politique ne remplace pas :

1.5.1 PII03 pour l’inventaire des traitements et la responsabilité relative à la base légale ;

1.5.2 PII06 pour le workflow complet relatif aux droits des personnes concernées ;

1.5.3 PII07 pour la méthodologie d’appréciation des risques relatifs à la vie privée et de DPIA ;

1.5.4 PII08 pour les points de contrôle de protection de la vie privée dès la conception et par défaut ;

1.5.5 PII09 pour les contrôles généraux de collecte, d’utilisation, de divulgation et de partage ;

1.5.6 PII10 pour la méthodologie générale de conservation, de suppression et d’élimination ;

1.5.7 PII12 pour la gouvernance générale du cycle de vie des sous-traitants, des sous-traitants ultérieurs et des tiers ;

1.5.8 PII13 pour l’évaluation des outils de transfert international ;

1.5.9 PII14 pour l’architecture complète de sécurité et de contrôle d’accès aux PII ;

1.5.10 PII15 pour le workflow de gestion des incidents et des violations ;

1.5.11 PII17 pour la maîtrise des informations documentées ;

1.5.12 PII18 pour la gouvernance de la surveillance, de l’audit et de l’amélioration du PIMS.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les services de sous-traitance et de sous-traitance ultérieure de PII dans le cloud soient exploités sur la base d'instructions documentées du client, d'un champ de traitement clairement défini, d'accords de sous-traitance ultérieure maîtrisés, de responsabilités appropriées en matière de sécurité cloud, d'emplacements et de routage de transferts documentés, d'obligations d'assistance au client, de support en cas de violation, de capacités de suppression et de restitution, ainsi que d'éléments de preuve compatibles avec les exigences d'audit.

2.2 La présente politique contribue à la préparation à la certification ISO/IEC 27701:2025 du PIMS pour les sous-traitants cloud et les sous-traitants ultérieurs cloud, tout en restant intégrée à l'ensemble de politiques PIMS existant et aux éléments de preuve canoniques.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 Définir le champ du traitement cloud de PII avant l'intégration du client ou toute modification substantielle.

3.1.2 Veiller à ce que les instructions du client soient enregistrées, revues et suivies.

3.1.3 Tenir à jour les éléments de preuve relatifs au sous-traitant cloud et au sous-traitant ultérieur dans les registres PIMS canoniques.

3.1.4 Définir les éléments de preuve relatifs à la responsabilité partagée, à l'isolement des locataires, aux accès, à la journalisation et aux emplacements sans dupliquer la politique de sécurité des PII.

3.1.5 Maîtriser les éléments de preuve relatifs à l'intégration, au changement, aux obligations répercutées et à la surveillance des sous-traitants ultérieurs.

3.1.6 Assister les clients pour les droits des personnes concernées, les DPIA, les demandes d'audit et la réponse aux violations.

3.1.7 Veiller à la conservation des éléments de preuve relatifs à la restitution, à la suppression, au transfert et à l'élimination lors de la sortie.

3.1.8 Surveiller les contrôles applicables au sous-traitant cloud et piloter les actions correctives au moyen de REG12.

4. Énoncés de politique

4.1 Champ du traitement cloud et instructions du client

4.1.1 [Processor] Privacy Lead / PIMS Manager doit enregistrer chaque service de traitement cloud de PII, le rôle de traitement du client, la source des instructions du client, les catégories de PII, les catégories de personnes concernées, la finalité du service, l'emplacement de traitement, la dépendance à un sous-traitant ultérieur, la dépendance à la suppression et l'indicateur de transfert dans REG02 et REG08 avant l'intégration du client ou toute modification substantielle du service.

4.1.2 [Processor] Process Owner / Business Owner doit enregistrer les instructions documentées du client relatives au traitement cloud de PII dans REG08 avant le début du traitement.

4.1.3 [Subprocessor] Process Owner / Business Owner doit enregistrer dans REG08 les instructions du sous-traitant amont ou approuvées par le client avant de traiter des PII en tant que sous-traitant ultérieur cloud.

4.1.4 [Processor] Privacy Lead / PIMS Manager doit enregistrer l'applicabilité des contrôles du sous-traitant cloud dans REG03 avant la mise à disposition ou la modification substantielle d'un nouveau service de traitement cloud de PII.

4.1.5 [Processor] Data Protection Officer / Privacy Advisor doit examiner dans REG12 toute instruction du client qui semble incompatible avec les obligations documentées du client, les exigences du PIMS ou le champ de service approuvé avant que l'organisation n'agisse sur cette instruction.

4.1.6 [Processor] Process Owner / Business Owner doit enregistrer dans REG12 tout traitement proposé de PII du client en dehors des instructions documentées du client et obtenir l'approbation de Privacy Lead / PIMS Manager avant que le traitement n'ait lieu.

4.2 Configuration cloud, isolement des locataires, accès et journalisation

4.2.1 [Processor] Information Security Lead doit enregistrer dans REG08 le périmètre de responsabilité partagée cloud pour l'accès aux PII, l'administration, la journalisation, la sauvegarde, le chiffrement, la gestion des vulnérabilités et la suppression avant l'intégration du client ou toute modification substantielle du service.

4.2.2 [Processor] System Owner / Application Owner doit valider dans REG12 les contrôles d'isolement des locataires ou de séparation des clients avant l'utilisation en production et après toute modification substantielle de l'architecture.

4.2.3 [Processor] System Owner / Application Owner doit accorder un accès administratif cloud aux PII du client uniquement après enregistrement dans REG12 du besoin métier approuvé, du périmètre d'accès, de la durée d'accès et de la fréquence de revue.

4.2.4 [Processor] Information Security Lead doit examiner dans REG12, au moins trimestriellement, les accès cloud à privilèges, les accès de support, les accès aux PII du client et la couverture de journalisation.

4.2.5 [Processor] System Owner / Application Owner doit valider dans REG12 la séparation des environnements de production, de préproduction, de test et de support pour les PII du client avant la mise en production et après toute modification substantielle de l'environnement.

4.2.6 [Processor] System Owner / Application Owner doit enregistrer les emplacements de sauvegarde, de réplication, de stockage des journaux et d'accès de support pour les PII des clients cloud dans REG02, REG08 ou REG09 avant d'activer ou de modifier ces emplacements.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exceptions

9.1 [Processor] Process Owner / Business Owner doit demander une exception relative au sous-traitant cloud dans REG12 avant l'intégration, la mise en production, le renouvellement ou la poursuite de l'utilisation lorsque les éléments de preuve requis relatifs aux instructions du client, aux sous-traitants ultérieurs, aux emplacements, aux accès, à la journalisation, à la suppression ou à l'interface incident sont incomplets.

9.2 [Processor] Data Protection Officer / Privacy Advisor doit examiner dans REG12 les demandes d'exception relatives au sous-traitant cloud présentant un enjeu significatif pour la vie privée avant approbation lorsque l'exception affecte les instructions du client, l'assistance aux personnes concernées, les transferts, les sous-traitants ultérieurs, la suppression, le support en cas de violation ou les PII à fort impact.

9.3 [Processor] Top Management doit approuver dans REG12 les exceptions à haut risque ou substantielles relatives au sous-traitant cloud avant leur entrée en vigueur.

9.4 [Processor] Privacy Lead / PIMS Manager doit attribuer dans REG12 une date d'expiration, un responsable de remédiation, une date de revue et une note relative au risque résiduel pour chaque exception approuvée avant approbation.

10. Mise en application

10.1 [Processor] Privacy Lead / PIMS Manager doit bloquer l'intégration du client, la mise à disposition du service, le renouvellement ou la poursuite du traitement lorsque les éléments de preuve requis dans REG02, REG03, REG08, REG09, REG10 ou REG12 sont manquants avant le début ou la poursuite du traitement.

10.2 [Processor] System Owner / Application Owner doit désactiver tout accès cloud non approuvé, toute utilisation de région non approuvée, toute réplication non approuvée, tout accès de support non approuvé ou tout flux de données vers un sous-traitant ultérieur non approuvé dans un délai d'un jour ouvrable après une décision de mise en application, et enregistrer l'achèvement dans REG08 ou REG12.

10.3 [Processor] Vendor / Procurement Owner doit suspendre tout nouveau traitement de PII par un sous-traitant ultérieur cloud non approuvé ou non conforme jusqu'à ce que les éléments de preuve d'action corrective dans REG08 soient complets.

10.4 [Processor] Incident Response Coordinator doit escalader les échéances manquées de notification d'incident au client dans REG10 et REG12 dans un délai d'un jour ouvrable après identification.

10.5 [Processor] Internal Audit / Compliance Reviewer doit vérifier dans REG12 l'efficacité des actions correctives pour les non-conformités majeures ou répétées relatives au sous-traitant cloud dans les 60 jours suivant la clôture de l'action corrective.

11. Revue et maintenance

11.1 [Processor] Privacy Lead / PIMS Manager doit revoir la présente politique dans REG12 annuellement et dans les 30 jours suivant une modification substantielle des obligations du sous-traitant cloud, de l'architecture cloud, de la gouvernance des sous-traitants ultérieurs, de l'assistance au client, de la capacité de suppression ou des exigences de certification.

11.2 [Processor] Vendor / Procurement Owner doit revoir les enregistrements relatifs aux sous-traitants ultérieurs cloud et aux dépendances à des services cloud dans REG08 au moins une fois par an et avant le renouvellement.

11.3 [Processor] System Owner / Application Owner doit revoir dans REG12 les éléments de preuve relatifs à l'isolement des locataires, aux accès à privilèges, à la journalisation, aux sauvegardes, à la réplication et à la suppression au moins une fois par an et après toute modification substantielle de l'architecture.

11.4 [Processor] Privacy Lead / PIMS Manager doit revoir les enregistrements REG09 relatifs aux emplacements cloud et au routage des transferts au moins une fois par an et dans les 15 jours ouvrables suivant une modification substantielle d'emplacement, d'accès de support, de sauvegarde ou de sous-traitant ultérieur.

11.5 [Processor] Privacy Lead / PIMS Manager doit mettre à jour REG03 dans les 15 jours ouvrables suivant les modifications approuvées de la politique qui affectent l'applicabilité des contrôles du sous-traitant cloud.

11.6 [All] Top Management doit approuver les révisions substantielles de la présente politique dans REG12 avant publication.

12. Politiques associées

12.1 La présente politique est appuyée par les politiques associées suivantes :

12.2 PII01 - Politique du système de management des informations relatives à la vie privée

12.3 PII02 - Politique relative aux rôles, responsabilités et à la responsabilité en matière de vie privée

12.4 PII03 - Politique relative à l'inventaire des traitements de PII et à la base légale

12.5 PII06 - Politique de gestion des droits des personnes concernées

12.6 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA

12.7 PII08 - Politique de protection de la vie privée dès la conception et par défaut

12.8 PII09 - Politique de collecte, d'utilisation, de divulgation et de partage des PII

12.9 PII10 - Politique de conservation, de suppression et d'élimination des PII

12.10 PII12 - Politique de gestion de la protection des données pour les sous-traitants, les sous-traitants ultérieurs et les tiers

12.11 PII13 - Politique de transfert international de PII

12.12 PII14 - Politique de sécurité et de contrôle d'accès aux PII

12.13 PII15 - Politique de gestion des incidents et violations relatifs aux PII

12.14 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS

12.15 PII18 - Politique de surveillance, d'audit et d'amélioration du PIMS

12.16 PII20 - Politique de protection de la vie privée des enfants

12.17 PII21 - Politique de protection de la vie privée relative à l'AI et à la prise de décision automatisée

12.18 PII22 - Politique de protection de la vie privée relative au marketing et aux cookies

12.19 PII24 - Politique de vidéosurveillance et de surveillance physique

13. Normes et référentiels de référence

13.1 La présente politique est mise en correspondance avec les normes et réglementations suivantes. Cette correspondance explique comment la politique soutient les exigences citées et identifie les clauses internes qui les mettent en œuvre ou les soutiennent.

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].