					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII21					Titre du document : **Politique relative à la vie privée pour l'IA et la prise de décision individuelle automatisée**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Informations documentées et maîtrise opérationnelle des éléments de preuve relatifs au traitement par IA, au profilage et à la prise de décision individuelle automatisée
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance, non-conformité et action corrective pour les contrôles de protection de la vie privée liés à l'IA
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalité, base légale, analyse d'impact relative à la vie privée et enregistrements du responsable du traitement
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Contrats de sous-traitants et responsabilités des responsables conjoints du traitement pour le traitement de PII lié à l'IA
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Obligations envers les personnes concernées et transparence du traitement lié à l'IA
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Opposition, accès, rectification, effacement, traitement des demandes et obligations relatives à la prise de décision

				individuelle automatisée
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limites de collecte, de traitement et de minimisation applicables aux entrées, sorties et données dérivées de l'IA
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Acheminement des transferts internationaux, divulgations et demandes de divulgation concernant la PII liée à l'IA
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Accord avec le sous-traitant, instructions documentées, assistance aux obligations du client et enregistrements
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Assistance du sous-traitant pour les obligations envers les personnes concernées, l'acheminement des transferts et la gestion des divulgations
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection des enregistrements et journalisation liés au traitement de PII associé à l'IA
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profilage, loyauté, transparence, limitation des finalités, minimisation, exactitude et responsabilité
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Licéité, données relevant de

				catégories particulières et mesures de protection applicables aux données relatives aux condamnations pénales ou aux infractions
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Informations transparentes, accès et informations utiles concernant la prise de décision individuelle automatisée
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Droits de rectification, d'effacement, de limitation, d'opposition et droits relatifs à la prise de décision individuelle automatisée
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Responsabilité du responsable du traitement, protection dès la conception/par défaut, responsables conjoints du traitement, sous-traitants, enregistrements, sécurité, DPIA et missions du DPO
GDPR	Article 44	Conditional	Referenced	Acheminement des transferts internationaux pour le traitement de PII lié à l'IA
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Principes relatifs à la finalité, à la collecte, à la minimisation, à l'utilisation, à la conservation, à la

				divulgation, à l'exactitude et à la qualité
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparence, participation individuelle, responsabilité, sécurité de l'information et conformité en matière de vie privée
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Bénéfice de la PIA, détermination du seuil et préparation de l'appréciation des risques relatifs à la vie privée liés à l'IA
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Contrôles relatifs à la finalité, à la collecte, à la minimisation, à l'utilisation, à la conservation, à la divulgation, à l'exactitude et à la participation des personnes concernées

1. Champ d'application

1.1 La présente politique définit les exigences obligatoires de protection de la vie privée applicables aux activités de traitement reposant sur l'intelligence artificielle, le profilage, la notation, la recommandation, l'aide à la décision et la prise de décision individuelle automatisée qui utilisent, infèrent, génèrent, divulguent ou traitent autrement de la PII dans le domaine d'application du PIMS.

1.2 La présente politique s'applique aux éléments suivants :

1.2.1 les systèmes, applications, modèles, services, workflows, moteurs de décision, outils de notation, systèmes de recommandation, modèles d'analyse et processus de prise de décision individuelle automatisée fondés sur l'IA qui traitent de la PII ;

1.2.2 le profilage, la segmentation, la classification, la prédiction, l'inférence, la personnalisation, le classement, l'éligibilité, la détection de fraude, la notation du risque, les décisions d'accès, l'évaluation liée à l'emploi, le profilage concernant les enfants, la personnalisation marketing et les traitements similaires lorsque de la PII est concernée ;

1.2.3 la PII liée à l'IA utilisée pour l'entraînement, les tests, la validation, l'ajustement, la surveillance, l'inférence en production, la revue des sorties, la mesure de performance, l'investigation d'incident ou le retrait d'un modèle ;

1.2.4 les contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur ;

1.2.5 les fournisseurs, sous-traitants, sous-traitants ultérieurs, destinataires de partage de données et circuits de transfert international liés à l'IA qui traitent de la PII.

1.3 La présente politique ne crée pas de cadre complet de gouvernance de l'IA, de système de management de l'IA, d'inventaire de l'IA, d'inventaire des modèles, de registre des risques liés aux modèles, de registre d'équité, de registre des algorithmes, de registre des incidents IA, de comité IA, de rôle de propriétaire de modèle, de rôle de propriétaire de système IA, de workflow de conseil juridique ni de formulaire d'approbation IA distinct.

1.4 La présente politique ne remplace pas les éléments suivants :

1.4.1 PII03 pour l'inventaire des traitements, la base légale et la responsabilité du ROPA ;

1.4.2 PII04 pour la gouvernance des mentions d'information ;

1.4.3 PII05 pour le consentement et la gestion des préférences ;

1.4.4 PII06 pour le workflow relatif aux droits des personnes concernées ;

1.4.5 PII07 pour l'appréciation des risques relatifs à la vie privée et la méthodologie DPIA ;

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

1.4.7 PII09 pour les contrôles relatifs à la collecte, à l'utilisation, à la divulgation et au partage ;

1.4.8 PII10 pour l'exécution de la conservation, de la suppression et de l'élimination ;

1.4.9 PII11 pour les contrôles d'exactitude et de qualité ;

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

1.4.11 PII13 pour les contrôles des transferts internationaux ;

1.4.12 PII14 pour la sécurité et le contrôle d'accès ;

1.4.13 PII15 pour la gestion des incidents et des violations ;

1.4.14 PII18 pour la surveillance, l'audit et l'amélioration ;

1.4.15 PII19 pour la vie privée des employés ;

1.4.16 PII20 pour la vie privée des enfants ;

1.4.17 PII22 pour la vie privée en matière de marketing et les cookies.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les activités d'IA, de profilage et de prise de décision individuelle automatisée impliquant de la PII soient identifiées, documentées, appréciées au regard des risques, transparentes, contestables, surveillées et maîtrisées au moyen du PIMS, sans créer de livrables justificatifs de gouvernance propres à l'IA faisant double emploi.

2.2 La présente politique garantit que les obligations de protection de la vie privée applicables au traitement de PII lié à l'IA sont étayées par REG02, REG04, REG06, REG07, REG08, REG09, REG10 et REG12.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 identifier dans REG02 les traitements d'IA, de profilage et de prise de décision individuelle automatisée impliquant de la PII ;

3.1.2 documenter dans REG02 les finalités liées à l'IA, la base légale, les catégories de PII, les sources de données, les données inférées, les sorties, les destinataires et les effets des décisions ;

3.1.3 déclencher l'examen préalable des risques relatifs à la vie privée et l'acheminement DPIA au moyen de REG04 ;

3.1.4 veiller à ce que les mentions d'information et les informations utiles liées à l'IA soient enregistrées dans REG07 ;

3.1.5 acheminer les demandes relatives aux droits, à l'opposition, à la revue humaine et à la contestabilité au moyen de REG06 ;

3.1.6 maîtriser les sous-traitants, sous-traitants ultérieurs, fournisseurs et dispositifs de partage de données liés à l'IA au moyen de REG08 ;

3.1.7 acheminer les transferts internationaux liés à l'IA au moyen de REG09 ;

3.1.8 escalader les incidents PII présumés liés à l'IA, les usages abusifs, les divulgations non autorisées et les résultats défavorables en matière de vie privée au moyen de REG10 et REG12 ;

3.1.9 enregistrer la surveillance, les exceptions, les non-conformités, les actions correctives et les améliorations dans REG12.

4. Énoncés de politique

4.1 Identification de l'IA, du profilage et de la prise de décision individuelle automatisée

4.1.1 [Controller] Lorsqu'un système, une application, un modèle, un workflow, un service ou un processus métier nouveau ou substantiellement modifié est proposé, le Process Owner / Business Owner doit déterminer s'il utilise l'IA, le profilage, la notation, la recommandation, l'aide à la décision ou la prise de décision individuelle automatisée impliquant de la PII et enregistrer cette détermination dans REG02.

4.1.2 [Controller] Avant le début du traitement de PII lié à l'IA, le Process Owner / Business Owner doit documenter dans REG02 la finalité du traitement, les catégories de PII, les catégories de personnes concernées, les sources de données, les catégories de données inférées ou dérivées, les catégories de sorties, les catégories de destinataires, la base légale et le lien avec la conservation.

4.1.3 [Controller] Avant l'utilisation en production du profilage, de la notation, de la recommandation, de l'aide à la décision ou de la prise de décision individuelle automatisée, le Process Owner / Business Owner doit documenter dans REG02 et REG04 le contexte

décisionnel, l'effet attendu sur les personnes concernées, l'intervention humaine et le circuit d'exercice des droits.

4.1.4 [Joint Controller] Avant qu'un traitement de PII lié à l'IA soit réalisé avec un responsable conjoint du traitement, le Privacy Lead / PIMS Manager doit documenter dans REG08 les responsabilités relatives à la définition des finalités, aux mentions d'information, au traitement des droits, à l'assistance DPIA, à la gouvernance des sous-traitants et à l'escalade des incidents.

4.1.5 [Processor] Avant de traiter de la PII au moyen d'un service lié à l'IA pour un client, le Process Owner / Business Owner doit confirmer que les instructions du client, les finalités autorisées, les usages interdits, le traitement des sorties et les obligations d'assistance sont documentés dans REG08.

4.1.6 [Both] Avant l'activation d'un traitement de PII lié à l'IA, le Privacy Lead / PIMS Manager doit confirmer que le traitement est relié aux éléments de preuve canoniques applicables et qu'aucun registre propre à l'IA distinct n'est créé en dehors de REG02, REG04, REG06, REG07, REG08, REG09, REG10 ou REG12.

4.2 Appréciation des risques relatifs à la vie privée et acheminement DPIA

4.2.1 [Controller] Avant le lancement ou la modification substantielle d'un traitement de PII lié à l'IA, le Privacy Lead / PIMS Manager doit réaliser l'examen préalable des risques relatifs à la vie privée et enregistrer la décision DPIA dans REG04.

4.2.2 [Conditional] Lorsque le traitement lié à l'IA implique un profilage, des décisions automatisées, une évaluation à grande échelle, des données relevant de catégories particulières, des données relatives aux infractions pénales, des personnes concernées vulnérables, une évaluation des employés, des enfants, une surveillance comportementale, des données de localisation, des données biométriques, une notation à fort impact ou des effets significatifs, le Data Protection Officer / Privacy Advisor doit examiner le risque relatif à la vie privée et enregistrer son avis dans REG04.

4.2.3 [Controller] Avant la mise en production d'un traitement de PII lié à l'IA, le Process Owner / Business Owner doit documenter les actions de traitement des risques, le statut du risque résiduel et les éléments de preuve d'aptitude à la mise en production dans REG04 ou REG12.

4.2.4 [Controller] Avant que de la PII soit réutilisée pour l'entraînement, les tests, la validation, l'ajustement, la surveillance ou l'amélioration d'un modèle d'IA pour une finalité nouvelle ou substantiellement modifiée, le Process Owner / Business Owner doit réaliser une revue relative à la vie privée et enregistrer la décision dans REG02 et REG04.

4.2.5 [Conditional] Lorsqu'un risque résiduel relatif à la vie privée demeure élevé après le traitement prévu, Top Management doit approuver, rejeter ou exiger un traitement supplémentaire avant l'utilisation en production et enregistrer la décision dans REG04 et REG12.

[... 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 [All] Avant de déroger à une exigence de protection de la vie privée liée à l'IA figurant dans la présente politique, le Process Owner / Business Owner demandeur doit soumettre dans REG12 une justification d'exception et les éléments de preuve des contrôles compensatoires.

9.2 [Conditional] Lorsqu'une exception affecte le profilage, la prise de décision individuelle automatisée, la revue humaine, la contestabilité, la transparence, le résultat DPIA, la notation à fort impact, le traitement concernant les enfants, le traitement concernant les employés, les restrictions

applicables aux sous-traitants ou les transferts internationaux, le Data Protection Officer / Privacy Advisor doit examiner l'exception et enregistrer son avis dans REG04 ou REG12.

9.3 [Conditional] Lorsqu'une exception crée ou maintient un risque résiduel élevé relatif à la vie privée, Top Management doit approuver ou rejeter l'exception et enregistrer la décision dans REG04 et REG12.

9.4 [All] Avant l'expiration d'une exception approuvée relative à la vie privée liée à l'IA, le Privacy Lead / PIMS Manager doit examiner le statut de clôture, de renouvellement ou d'action corrective et enregistrer le résultat dans REG12.

10. Application de la politique

10.1 [All] Lorsqu'une non-conformité à la présente politique est identifiée, le Privacy Lead / PIMS Manager doit enregistrer la non-conformité et l'action corrective dans REG12.

10.2 [Both] Lorsqu'un traitement, une divulgation, un accès, un usage abusif de modèle, une défaillance dans l'exercice des droits ou un résultat défavorable en matière de vie privée concernant de la PII liée à l'IA est suspecté comme non autorisé, l'Incident Response Coordinator doit lancer l'escalade d'incident et enregistrer les éléments de preuve dans REG10 et REG12.

10.3 [Both] Lorsqu'un sous-traitant, sous-traitant ultérieur, fournisseur ou destinataire de partage de données ne satisfait pas aux obligations de protection de la vie privée liées à l'IA, le Vendor / Procurement Owner doit enregistrer l'action de remédiation, d'escalade ou de résiliation dans REG08 et REG12.

10.4 [All] Lorsque des non-conformités répétées ou systémiques liées à l'IA en matière de vie privée surviennent, Top Management doit examiner le problème et enregistrer l'action de direction dans REG12.

11. Revue et maintenance

11.1 [All] Au moins une fois par an, le Privacy Lead / PIMS Manager doit revoir la présente politique afin de vérifier qu'elle demeure appropriée et enregistrer le résultat de la revue dans REG12.

11.2 [Conditional] Lorsque les lois, services, modèles, sources de données, pratiques de profilage, logiques de prise de décision individuelle automatisée, dispositifs fournisseurs, circuits de transfert ou risques relatifs à la vie privée changent substantiellement, le Privacy Lead / PIMS Manager doit revoir les contrôles de protection de la vie privée liés à l'IA affectés et enregistrer le résultat dans REG02, REG04 ou REG12.

11.3 [Controller] Au moins une fois par an et après toute modification substantielle du parcours utilisateur lié à l'IA, le Process Owner / Business Owner doit revoir les éléments de preuve relatifs à la transparence, aux informations utiles, à la revue humaine et au circuit d'exercice des droits, et enregistrer la revue dans REG06 et REG07.

11.4 [All] Après la clôture des actions correctives relatives à la vie privée liées à l'IA, l'Internal Audit / Compliance Reviewer doit vérifier leur efficacité et enregistrer les éléments de preuve de vérification dans REG12.

12. Politiques associées

12.1 PII01 - Politique relative au système de management des informations relatives à la vie privée

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

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

12.4 PII04 - Politique relative aux mentions d'information et à la transparence

12.5 PII05 - Politique relative au consentement et à la gestion des préférences

12.6 PII06 - Politique relative à la gestion des droits des personnes concernées

12.7 PII07 - Politique relative à l'appréciation des risques relatifs à la vie privée et à la DPIA

12.8 PII08 - Politique relative à la protection de la vie privée dès la conception et par défaut

12.9 PII09 - Politique relative à la collecte, l'utilisation, la divulgation et le partage de PII

12.10 PII10 - Politique relative à la conservation, la suppression et l'élimination de PII

12.11 PII11 - Politique relative à l'exactitude et à la qualité de PII

12.12 PII12 - Politique relative à la gestion de la vie privée des sous-traitants, sous-traitants ultérieurs et tiers

12.13 PII13 - Politique relative aux transferts internationaux de PII

12.14 PII14 - Politique relative à la sécurité et au contrôle d'accès de PII

12.15 PII15 - Politique relative à la gestion des incidents et violations de PII

12.16 PII17 - Politique relative aux informations documentées et à la gestion des éléments de preuve du PIMS

12.17 PII18 - Politique relative à la surveillance, l'audit et l'amélioration du PIMS

12.18 PII19 - Politique relative à la vie privée des employés

12.19 PII20 - Politique relative à la vie privée des enfants

12.20 PII22 - Politique relative à la vie privée en matière de marketing et aux cookies

13. Normes et référentiels de référence

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].