					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII10					Titre du document : **Politique de conservation, de suppression et d'élimination des PII**							
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	Éléments de preuve documentés de conservation et contrôle opérationnel
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance, non-conformité et action corrective
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Responsabilité conjointe et registres des activités de traitement
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Appui à l'exécution de l'effacement
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Conservation, suppression et élimination
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Instructions du client et registres du sous-traitant
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Appui à la suppression et capacité d'élimination
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Élimination des supports et gestion des sauvegardes
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Limitation de la conservation et responsabilité
GDPR	Article 17	Controller	Supporting	Appui à l'exécution de l'effacement
GDPR	Article 24	Controller	Supporting	Mesures du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Répartition de la responsabilité conjointe

GDPR	Article 28	Processor	Supporting	Suppression et restitution par le sous-traitant
GDPR	Article 30	Both	Supporting	Registres des activités de traitement
GDPR	Article 32	Both	Supporting	Traitement sécurisé et appui à l'élimination
ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimisation, limitation de la conservation et responsabilité
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Contrôles de conservation et d'effacement des fichiers temporaires
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	Both	Primary	Cadre de suppression et documentation
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Durées de suppression et règles de suppression
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	Both	Primary	Mise en œuvre et exceptions
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Responsabilités et gouvernance de la mise en œuvre
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Intégration des risques relatifs à la vie privée
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Élimination sécurisée et suppression des informations

1. Champ d'application

1.1 La présente politique définit les exigences de l'organisation relatives à la définition, à la revue, à l'exécution et à la conservation des éléments de preuve concernant la conservation, la suppression, l'anonymisation, la désidentification, la restitution, le transfert et l'élimination des PII.

1.2 La présente politique s'applique aux PII traitées dans des contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur, y compris les PII conservées dans les systèmes en production, les archives, les copies de sauvegarde, les réplicas, les journaux, les environnements de préproduction, les fichiers temporaires, les documents papier et les supports de stockage.

1.3 La présente politique s'applique aux obligations de conservation et de suppression découlant des finalités de traitement approuvées, des enregistrements de base légale, des instructions du responsable du traitement, des exigences contractuelles, des suites données aux demandes d'effacement des personnes concernées, de la sortie de service, de l'élimination des supports de stockage et des constats issus de la surveillance du PIMS.

1.4 La présente politique ne définit pas le choix de la base légale, le contenu des mentions d'information, la gestion complète des droits des personnes concernées, la gouvernance du cycle de vie des sous-traitants, les mécanismes de transfert international, l'architecture des contrôles de sécurité, le processus de réponse aux incidents ni la méthodologie d'audit du PIMS. Ces contrôles sont traités dans les politiques associées.

1.5 Aux fins de la présente politique, une modification substantielle désigne toute modification de la finalité du traitement, de la catégorie de PII, de la catégorie de personne concernée, de l'emplacement de stockage du système, de la loi ou du contrat applicable à la conservation, de l'instruction du client, de l'architecture de sauvegarde, de l'approche d'archivage, de la méthode d'élimination, du dispositif avec un sous-traitant ou un sous-traitant ultérieur, du workflow d'effacement ou du domaine de certification du PIMS qui affecte la conservation, la suppression ou l'élimination.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les PII ne soient conservées que pour des finalités et des durées approuvées, qu'elles soient supprimées ou autrement éliminées lorsqu'elles ne sont plus nécessaires, et qu'elles soient appuyées par des éléments de preuve compatibles avec les exigences d'audit.

2.2 La présente politique permet à l'organisation de démontrer la limitation de la conservation, une gouvernance responsable de la conservation, une exécution maîtrisée de la suppression, une élimination sécurisée, l'alignement sur les instructions du client pour les activités de sous-traitance, la maîtrise des exceptions et l'amélioration continue, sans créer de registre de suppression distinct.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir la propriété des règles de conservation et les métadonnées de conservation requises ;

3.1.2 veiller à ce que les règles de conservation soient enregistrées dans l'inventaire des traitements de PII / ROPA ;

3.1.3 veiller à ce que les actions de suppression des sous-traitants et des sous-traitants ultérieurs soient fondées sur l'instruction du client ou sur le contrat ;

3.1.4 veiller à ce que les PII arrivées à expiration soient supprimées, restituées, transférées, anonymisées, désidentifiées ou éliminées selon des méthodes approuvées ;

3.1.5 distinguer les systèmes en production, les archives, les sauvegardes, les réplicas, les journaux, les zones de préproduction et les fichiers temporaires ;

3.1.6 veiller à ce que les éléments de preuve relatifs à la suppression et à l'élimination soient conservés dans les objets de preuve PIMS canoniques ;

3.1.7 veiller à ce que les exceptions à la conservation soient limitées dans le temps, approuvées et revues ;

3.1.8 intégrer la surveillance de la conservation et de la suppression à la non-conformité, à l'action corrective et à l'amélioration.

4. Énoncés de politique

4.1 Attribution des règles de conservation

4.1.1 [Controller] The Process Owner / Business Owner MUST attribuer une règle de conservation documentée à chaque activité de traitement du responsable du traitement dans REG02 avant le début de l'activité de traitement.

4.1.2 [Joint Controller] The Process Owner / Business Owner MUST enregistrer la répartition des responsabilités en matière de conservation et de suppression entre responsables conjoints du traitement dans REG02 et REG08 avant le début ou la modification du traitement conjoint.

4.1.3 [Processor] The Vendor / Procurement Owner MUST enregistrer les instructions du client relatives à la conservation, à la restitution, au transfert ou à la suppression pour les activités du sous-traitant dans REG08 avant le début ou la modification du traitement par le sous-traitant.

4.1.4 [Subprocessor] The Vendor / Procurement Owner MUST enregistrer les exigences de répercussion relatives à la conservation, à la restitution, au transfert ou à la suppression applicables au sous-traitant ultérieur dans REG08 avant l'intégration du sous-traitant ultérieur ou la modification des instructions.

4.1.5 [Both] The Privacy Lead / PIMS Manager MUST vérifier que chaque règle de conservation approuvée dans REG02 comprend la durée de conservation, le déclencheur de départ, le propriétaire, la justification, le sort final et la prochaine date de revue avant que la règle ne soit approuvée.

4.1.6 [Both] The Data Protection Officer / Privacy Advisor MUST enregistrer son avis dans REG02 ou REG12 avant l'approbation de toute règle de conservation impliquant un conflit juridique, un traitement à haut risque, des PII de catégorie particulière ou une conservation au-delà de la finalité initiale du traitement.

4.2 Revue et limitation de la conservation

4.2.1 [Both] The Process Owner / Business Owner MUST revoir les règles de conservation attribuées dans REG02 au moins une fois par an et dans les 30 jours suivant une modification substantielle.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST approuver ou rejeter les règles de conservation nouvelles ou modifiées dans REG02 dans les 10 jours ouvrés suivant leur soumission.

4.2.3 [Both] The System Owner / Application Owner MUST confirmer la méthode d'application technique ou manuelle de chaque règle de conservation dans REG02 avant la mise en production et lors de chaque revue annuelle de la conservation.

4.2.4 [Controller] The Process Owner / Business Owner MUST restreindre l'utilisation active des PII conservées uniquement pour des raisons légales, contractuelles, d'audit ou de litige dans REG02 dans les cinq jours ouvrés suivant l'identification de la condition de restriction.

4.2.5 [Both] The Privacy Lead / PIMS Manager MUST enregistrer tout risque non résolu de conservation excessive ou toute revue de conservation en retard dans REG12 dans les cinq jours ouvrés suivant son identification.

[... 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

9.1.1 [All] The Process Owner / Business Owner MUST soumettre toute demande visant à conserver des PII au-delà de la règle de conservation REG02 approuvée dans REG12 avant que l'exception ne devienne active.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST approuver ou rejeter les demandes d'exception à la conservation dans REG12 avant que l'exception ne devienne active.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST enregistrer son avis dans REG12 avant l'approbation de toute exception impliquant un conflit juridique, un refus d'effacement, des PII à haut risque, un partage externe ou un impact sur la certification.

9.1.4 [All] Top Management MUST approuver dans REG12 les exceptions à la conservation dépassant 90 jours, affectant un traitement à haut risque ou affectant l'assurance externe avant que l'exception ne devienne active.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST attribuer un propriétaire, une date d'expiration, un contrôle compensatoire et une fréquence de revue dans REG12 pour chaque exception approuvée relative à la conservation, à la suppression ou à l'élimination.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST revoir chaque exception ouverte dans REG12 au moins une fois par mois jusqu'à sa clôture.

9.1.7 [All] The Process Owner / Business Owner MUST clôturer ou renouveler chaque exception dans REG12 avant la date d'expiration de l'exception.

10. Application

10.1.1 [All] The Privacy Lead / PIMS Manager MUST enregistrer une non-conformité dans REG12 dans les cinq jours ouvrés suivant l'identification de métadonnées de conservation manquantes, d'une revue de conservation en retard, d'une conservation non étayée, d'une action de sort final manquée ou d'éléments de preuve manquants.

10.1.2 [All] The System Owner / Application Owner MUST suspendre toute nouvelle utilisation en production d'une activité de traitement dans REG12 lorsque les contrôles techniques de conservation requis sont absents avant la mise en production.

10.1.3 [All] The Process Owner / Business Owner MUST arrêter l'utilisation active non approuvée de PII conservées uniquement pour des raisons légales, contractuelles, d'audit ou de litige dans les cinq jours ouvrés et enregistrer l'action dans REG02 ou REG12.

10.1.4 [Processor] The Vendor / Procurement Owner MUST escalader les actions de sort final ordonnées par le client et en retard dans REG08 et REG12 dans les cinq jours ouvrés suivant le non-respect de l'échéance contractuelle.

10.1.5 [Subprocessor] The Vendor / Procurement Owner MUST escalader les éléments de preuve de sort final manquants du sous-traitant ultérieur dans REG08 et REG12 dans les cinq jours ouvrés suivant le non-respect de l'échéance contractuelle de production des preuves.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST vérifier l'efficacité des actions correctives relatives aux non-conformités de conservation, de suppression et d'élimination dans REG12 lors du prochain audit planifié ou dans les 60 jours suivant la clôture, selon la première éventualité.

10.1.7 [Conditional] The Incident Response Coordinator MUST initier la gestion dans REG10 lorsqu'une non-conformité de conservation, de suppression ou d'élimination indique une suspicion d'incident PII.

11. Revue et maintien à jour

11.1.1 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique chaque année et enregistrer le résultat de la revue dans REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique dans les 30 jours suivant toute modification substantielle de la loi relative à la conservation, de la finalité du traitement, de l'instruction du sous-traitant, de l'architecture système, de l'architecture de sauvegarde, de l'approche d'archivage, du workflow d'effacement, du processus d'élimination ou des exigences de certification PIMS.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST revoir les modifications de la présente politique ayant un enjeu significatif pour la vie privée dans REG12 avant approbation.

11.1.4 [All] Top Management MUST approuver les modifications substantielles de la présente politique dans REG12 avant publication.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST enregistrer la communication des modifications approuvées de la politique dans REG11 dans les 30 jours suivant la publication.

12. Politiques associées

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

12.2 PII01 - Politique relative au 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 protection des données

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

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

12.6 PII06 - Politique de gestion des droits des personnes concernées

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

12.8 PII09 - Politique relative à la collecte, à l'utilisation, à la divulgation et au partage des PII

12.9 PII12 - Politique de management de la protection des données des sous-traitants, sous-traitants ultérieurs et tiers

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

12.11 PII15 - Politique de gestion des incidents et violations concernant les PII

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

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

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 appuient.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mise en correspondance avec les éléments de preuve documentés de conservation, la planification opérationnelle, les métadonnées de conservation, les éléments de preuve de mise en œuvre et les enregistrements d'exécution du cycle de vie. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Mise en correspondance avec la surveillance, les indicateurs, la revue des actions en retard, la non-conformité et l'action corrective relatives aux contrôles de conservation, de suppression et d'élimination. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].

13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Mise en correspondance avec les éléments de preuve de responsabilité entre responsables conjoints du traitement et les registres des activités de traitement du responsable du traitement contenant les métadonnées de conservation et de sort final. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].

13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Mise en correspondance avec l'appui à l'exécution de l'effacement, l'orientation de l'évaluation de suppression et l'articulation avec les éléments de preuve de tiers lorsque les suites données à l'effacement exigent une action. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Mise en correspondance avec la suppression ou la désidentification à la fin du traitement, la gestion des fichiers temporaires, la limitation de la conservation et les contrôles documentés de sort final. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].

13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mise en correspondance avec les accords clients du sous-traitant, les finalités documentées du client et les registres des activités de traitement du sous-traitant. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].

13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Mise en correspondance avec l'appui du sous-traitant aux obligations du client, la gestion des fichiers temporaires et la capacité de restitution, de transfert ou de sort final. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].

13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Mise en correspondance avec la gestion du cycle de vie des supports de stockage, les contrôles de réutilisation ou de libération des équipements et la gestion des sauvegardes pour les PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].

13.3 GDPR

13.3.1 **Article 5(1)(e); Article 5(2)** - Mise en correspondance avec la limitation de la conservation, la responsabilité en matière de conservation, les métadonnées de conservation approuvées, les éléments de preuve et la revue. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].

13.3.2 **Article 17** - Mise en correspondance avec l'orientation des suites approuvées de l'effacement, les éléments de preuve d'exécution et l'escalade d'incident lorsque des défaillances des contrôles d'effacement indiquent une suspicion d'incident PII. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].

13.3.3 **Article 24** - Mise en correspondance avec la gouvernance du responsable du traitement, les mesures de responsabilité, les revues, les exceptions, l'action corrective et le maintien à jour de la politique. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].

13.3.4 **Article 26** - Mise en correspondance avec la répartition des responsabilités entre responsables conjoints du traitement en matière de conservation et de suppression. Addressed by clauses [4.1.2; 6.1.4].

13.3.5 **Article 28** - Mise en correspondance avec l'alignement des instructions des sous-traitants et sous-traitants ultérieurs, la restitution, le transfert, le sort final, les éléments de preuve et l'escalade. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].

13.3.6 **Article 30** - Mise en correspondance avec les métadonnées de conservation et de sort final dans les registres des activités de traitement pour les activités du responsable du traitement et du sous-traitant. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Mise en correspondance avec la gestion opérationnelle sécurisée des PII conservées, l'application technique, le contrôle des supports de stockage, la gestion des sauvegardes et l'escalade des incidents. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Mise en correspondance avec la minimisation des données, la limitation de l'utilisation et de la conservation, le sort final lorsque les données ne sont plus nécessaires, la restriction des PII conservées et les éléments de preuve de responsabilité. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Mise en correspondance avec la conservation limitée dans le temps, le sort final, l'application automatisée ou manuelle et la gestion des fichiers temporaires. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Mise en correspondance avec la gouvernance du cadre de suppression, le regroupement des PII, les durées de conservation et de suppression, la distinction entre archives et sauvegardes, la structure des règles de suppression et les exigences de procédure documentée. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Mise en correspondance avec la spécification des périodes régulières de suppression, l'identification des périodes standard de suppression et l'attribution des règles de suppression aux activités de traitement de PII. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Mise en correspondance avec les exigences de mise en œuvre pour les systèmes, les processus manuels, les aspects à l'échelle de l'organisation, les sous-traitants, la gestion de la récupération et la gestion des exceptions. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Mise en correspondance avec l'attribution des rôles, la documentation, l'intégration opérationnelle, l'audit et la gouvernance de la mise en œuvre de la conservation, de la suppression et de l'élimination. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Mise en correspondance avec la gouvernance fondée sur les risques relatifs à la vie privée, la sensibilisation de la direction, l'intégration du risque relatif à la vie privée dans le PIMS et le contexte de risque lié à la conservation. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Mise en correspondance avec la suppression des informations, l'achèvement maîtrisé du cycle de vie, la libération des supports de stockage et les éléments de preuve du sort final. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].