					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII17					Titre du document : **Politique de gestion des informations documentées et des éléments de preuve du PIMS**							
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 6.1.3	Both	Supporting	Informations documentées de la Déclaration d'applicabilité
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informations documentées du PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Contrôle des éléments de preuve opérationnels
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Éléments de preuve de surveillance
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Éléments probants d'audit
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Éléments de preuve de revue de direction
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Éléments de preuve de non-conformité et d'action corrective
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registres de traitement du responsable du traitement
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Éléments de preuve relatifs aux accords et instructions du sous-traitant
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Protection des enregistrements
GDPR	Article 5(2)	Controller	Supporting	Éléments de preuve de responsabilité
GDPR	Article 24	Controller	Supporting	Mesures et éléments de preuve du responsable du traitement

GDPR	Article 28	Both	Supporting	Documentation du sous-traitant
GDPR	Article 30	Both	Supporting	Registres des traitements
GDPR	Article 32	Both	Supporting	Protection des éléments de preuve
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Éléments de preuve de conformité à la vie privée
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Protection des enregistrements
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Contrôle des informations documentées
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Protection des enregistrements
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Protection de la vie privée et des PII

1. Champ d'application

1.1 La présente politique définit les exigences obligatoires relatives à la création, à l'approbation, à la gestion des versions, à la protection, à la conservation, à la récupération, à la traduction, au retrait et à la constitution d'éléments de preuve concernant les informations documentées du PIMS.

1.2 La présente politique s'applique aux politiques PIMS, aux registres, aux approbations documentées, aux enregistrements constituant des éléments de preuve, aux éléments probants d'audit, aux enregistrements de revue de direction, aux éléments de preuve d'action corrective et aux traductions contrôlées utilisés pour démontrer la conformité du PIMS.

1.3 La présente politique s'applique aux contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur.

1.4 La présente politique ne crée pas de registre distinct de contrôle documentaire. Les éléments de preuve relatifs au contrôle des informations documentées sont tenus au moyen des éléments de preuve PIMS de référence REG01 à REG12, REG03 et REG12 étant utilisés pour les éléments de preuve relatifs à l'applicabilité des contrôles, à l'audit, aux non-conformités, aux actions correctives et à l'amélioration.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les informations documentées du PIMS soient exactes, contrôlées, accessibles aux utilisateurs autorisés, protégées contre toute modification ou divulgation non autorisée, conservées à des fins d'auditabilité et retirées lorsqu'elles deviennent obsolètes.

2.2 La présente politique soutient la préparation à la certification en veillant à ce que les éléments de preuve nécessaires pour démontrer la conformité du PIMS puissent être localisés, vérifiés, récupérés et reliés aux politiques, contrôles, activités de traitement, risques, audits et actions correctives applicables.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir les exigences de contrôle des informations documentées du PIMS ;

3.1.2 maintenir l'intégrité des éléments de preuve dans REG01 à REG12 ;

3.1.3 veiller à ce que l'approbation des politiques et des éléments de preuve soit traçable ;

3.1.4 veiller à ce que l'historique des versions et les décisions de retrait soient documentés ;

3.1.5 relier les éléments de preuve du PIMS à la Déclaration d'applicabilité et aux correspondances avec les politiques ;

3.1.6 contrôler l'accès aux documents PIMS et aux enregistrements constituant des éléments de preuve ;

3.1.7 soutenir la gestion des versions des politiques et des éléments de preuve multilingues ;

3.1.8 permettre la récupération en temps utile des éléments probants d'audit ;

3.1.9 éviter une bureaucratie inutile de contrôle documentaire ;

3.1.10 conserver des enregistrements compatibles avec les exigences d'audit aux fins de certification, d'assurance demandée par les clients et d'amélioration continue.

4. Énoncés de politique

4.1 Contrôle des informations documentées du PIMS

4.1.1 [All] The Privacy Lead / PIMS Manager MUST tenir un index des informations documentées du PIMS dans REG12 avant la publication initiale du PIMS puis trimestriellement.

4.1.2 [All] The Process Owner / Business Owner MUST identifier dans REG02 les informations documentées requises pour chaque activité de traitement de PII dont il est responsable avant le début de l'activité de traitement puis annuellement.

4.1.3 [All] The Privacy Lead / PIMS Manager MUST relier les politiques, contrôles et obligations relatives aux éléments de preuve applicables du PIMS à REG03 avant chaque publication de politique et dans un délai de 15 jours ouvrables suivant toute modification substantielle de l'applicabilité des contrôles.

4.1.4 [All] The Privacy Lead / PIMS Manager MUST attribuer un niveau d'accès et une classification de sensibilité des éléments de preuve à chaque catégorie d'informations documentées du PIMS dans REG12 avant que la catégorie ne soit utilisée.

4.2 Création, approbation, gestion des versions et publication

4.2.1 [All] The Privacy Lead / PIMS Manager MUST attribuer un identifiant de document, un propriétaire, un numéro de version, un statut d'approbation, une date d'entrée en vigueur et une date de revue dans REG12 avant de publier des informations documentées du PIMS.

4.2.2 [All] Top Management MUST approuver les politiques principales du PIMS et les modifications substantielles des politiques dans REG12 avant publication.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST approuver les modèles d'éléments de preuve du PIMS ou les sections de registre intégrées dans REG12 avant leur utilisation opérationnelle.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST consigner l'historique des versions et la justification des modifications dans REG12 avant la publication d'informations documentées du PIMS mises à jour.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST consigner la communication des modifications approuvées des informations documentées du PIMS dans REG11 dans un délai de 30 jours suivant la publication.

[... 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 demander dans REG12 toute exception relative aux informations documentées ou au contrôle des éléments de preuve avant de s'écarter de la présente politique.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST évaluer chaque exception relative aux informations documentées ou au contrôle des éléments de preuve dans REG12 dans un délai de 10 jours ouvrables suivant la demande.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST consigner ses avis dans REG12 avant l'approbation de toute exception impliquant la divulgation d'éléments de preuve contenant des PII, une divergence de traduction, un conflit de conservation ou une limitation des éléments probants d'audit.

9.1.4 [All] Top Management MUST approuver dans REG12 les exceptions relatives aux informations documentées dépassant 30 jours ou affectant la certification, un traitement à haut risque ou une assurance externe avant que l'exception ne prenne effet.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST fixer dans REG12, pour chaque exception approuvée relative aux informations documentées ou au contrôle des éléments de preuve, une date d'expiration n'excédant pas 90 jours.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST clôturer ou réévaluer chaque exception relative aux informations documentées ou au contrôle des éléments de preuve dans REG12 dans un délai de cinq jours ouvrables suivant son expiration.

10. Application de la politique

10.1.1 [All] The Privacy Lead / PIMS Manager MUST consigner comme non-conformité dans REG12 toute information documentée du PIMS manquante, inexacte, non contrôlée, obsolète ou irrécupérable dans un délai de cinq jours ouvrables suivant son identification.

10.1.2 [All] The Privacy Lead / PIMS Manager MUST empêcher la publication d'informations documentées du PIMS lorsque les éléments de preuve requis relatifs à l'approbation, à la version, au propriétaire ou à la date d'entrée en vigueur sont absents de REG12.

10.1.3 [All] The Process Owner / Business Owner MUST empêcher la soumission en audit d'éléments de preuve relatifs au traitement lorsque les éléments de preuve requis relatifs au propriétaire, à la date, au statut ou à l'approbation sont absents de REG02.

10.1.4 [All] The System Owner / Application Owner MUST supprimer tout accès non autorisé aux référentiels d'informations documentées du PIMS et consigner la suppression dans REG12 dans un délai d'un jour ouvrable suivant son identification.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST vérifier l'efficacité des actions correctives relatives aux non-conformités portant sur les informations documentées dans REG12 lors du prochain audit programmé ou dans un délai de 60 jours suivant la clôture, selon la première échéance.

11. Revue et maintenance

11.1.1 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique annuellement et dans un délai de 30 jours suivant toute modification substantielle des exigences relatives aux informations documentées du PIMS.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique dans un délai de 30 jours suivant un constat d'audit majeur, une non-conformité de certification, une modification de plateforme de référentiel ou une modification du processus de publication multilingue.

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

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

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

12. Politiques associées

12.1 La présente politique est soutenue 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 d'inventaire des traitements de PII et de base légale

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

12.6 PII05 - Politique de gestion du consentement et des préférences

12.7 PII06 - Politique de gestion des droits des personnes concernées

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

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

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

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

12.12 PII11 - Politique d'exactitude et de qualité des PII

12.13 PII12 - Politique de gestion de la protection des données applicable aux sous-traitants, sous-traitants ultérieurs et tiers

12.14 PII13 - Politique de transfert international de données à caractère personnel

12.15 PII14 - Politique de sécurité et de contrôle d'accès des PII

12.16 PII15 - Politique de gestion des incidents et violations de PII

12.17 PII16 - Politique de formation, de sensibilisation et de compétence en matière de vie privée

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

13. Normes et référentiels de référence

13.1 La présente politique est mappée aux normes et réglementations suivantes. La 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

13.2.1 **Clause 6.1.3** - Mappée à la tenue de la Déclaration d'applicabilité du PIMS, des enregistrements d'applicabilité des contrôles et du lien entre politiques et éléments de preuve. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mappée à l'identification des informations documentées, à l'approbation, à la gestion des versions, à l'accès, à la récupération, à la préservation, au retrait, au lien entre versions traduites et aux métadonnées de conservation. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mappée aux éléments de preuve de planification et de contrôle opérationnels concernant les enregistrements de traitement, les modèles d'éléments de preuve, la qualité des éléments de preuve opérationnels et les éléments de preuve fournis par des tiers. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mappée à la tenue d'éléments de preuve documentés concernant la mesure, la performance de récupération, les lacunes des éléments de preuve, les incohérences de traduction et l'achèvement de la revue d'accès aux référentiels. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mappée à la récupération des éléments probants d'audit, à l'échantillonnage d'audit, à la traçabilité des éléments probants d'audit et aux constats d'audit relatifs au contrôle des informations documentées. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mappée aux éléments de preuve de revue de direction, à la prise en compte du contrôle des informations documentées lors de la revue de direction et à la revue par Top Management de la performance du contrôle des éléments de preuve. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mappée aux non-conformités relatives aux informations documentées, aux actions correctives, à la gestion des exceptions, à la clôture et à la vérification de l'efficacité. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mappée aux registres de traitement du responsable du traitement, aux enregistrements de responsabilité, à la qualité des éléments de preuve relatifs au traitement et à la conservation des éléments de preuve soutenant les obligations du responsable du traitement. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mappée aux accords du sous-traitant, aux instructions du client, aux éléments de preuve fournis par des tiers et au contrôle des éléments de preuve relatifs à la relation avec le sous-traitant. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mappée à la protection des enregistrements du PIMS contre la perte, la modification non autorisée, l'accès non autorisé, la communication non autorisée et l'élimination inappropriée. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappé aux éléments de preuve de responsabilité, à la traçabilité des éléments de preuve, à la récupération des éléments de preuve, aux enregistrements de non-conformité et aux enregistrements compatibles avec les exigences d'audit démontrant la conformité. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mappé aux éléments de preuve de gouvernance du responsable du traitement, aux enregistrements d'approbation, au contrôle des politiques, aux mesures de responsabilité, à la revue documentée et à la supervision par Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mappé à la documentation des sous-traitants et sous-traitants ultérieurs, aux éléments de preuve des instructions du client, aux éléments de preuve de processus fournis par des tiers et au contrôle de la divulgation des éléments de preuve. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mappé aux éléments de preuve des registres de traitement, aux exigences de qualité des éléments de preuve, aux références d'activités de traitement et aux métadonnées de propriétaire/statut des éléments de preuve relatifs au traitement. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mappé à la protection des référentiels d'éléments de preuve, aux restrictions d'accès, aux approbations d'accès, à la revue de protection des référentiels et à la suppression des accès non autorisés. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mappée aux éléments de preuve de conformité à la vie privée, à la récupération des éléments probants d'audit, à la traçabilité des éléments de preuve, au soutien des revues indépendantes et aux éléments de preuve d'action corrective. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mappée à la protection des enregistrements liés aux PII, à la préservation des enregistrements et aux contrôles d'accès et de suppression des référentiels d'éléments de preuve. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mappée à l'identification des informations documentées, à l'approbation, à la disponibilité, à la protection, à la gestion des versions, à la conservation, au sort final et au contrôle des informations documentées exigées par des tiers. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mappé à la protection des enregistrements PIMS contre la perte, la destruction, la falsification, l'accès non autorisé, la communication non autorisée et l'élimination inappropriée. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mappé à la protection de la vie privée et des PII dans les informations documentées, les référentiels d'éléments de preuve, les divulgations et les enregistrements à accès contrôlé. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].