					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII16					Titre du document : **Politique de formation, de sensibilisation et de compétence en matière de vie privée**							
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 / Mesure / Article	Applicabilité	Type de couverture	Commentaire
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Compétence et sensibilisation
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Communication et éléments de preuve documentés
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Maîtrise opérationnelle, mesure et amélioration
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Sensibilisation, éducation et formation au traitement des PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Responsabilité, gouvernance des sous-traitants, sécurité et missions du DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Compétence, sensibilisation et formation
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Recommandations relatives à la sensibilisation, à l'éducation et à la formation
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Sécurité de l'information et conformité en matière de vie privée

1. Champ d'application

1.1 La présente politique définit les exigences de l'organisation relatives à la formation, à la sensibilisation et à la compétence en matière de vie privée au sein du système de management des informations relatives à la vie privée.

1.2 La présente politique s'applique au personnel, aux contractants, au personnel temporaire, aux tiers pertinents, aux sous-traitants, aux sous-traitants ultérieurs et aux autres parties intéressées dont les travaux peuvent affecter le traitement des PII, la performance du PIMS, les droits des personnes concernées, les risques relatifs à la vie privée, la sécurité de l'information liée aux PII, les instructions du sous-traitant, les incidents relatifs à la vie privée, les informations documentées ou les éléments de preuve de conformité.

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 couvre :

1.4.1 l'identification des publics cibles de la formation à la vie privée ;

1.4.2 la formation d'intégration ;

1.4.3 la formation de rappel annuelle ;

1.4.4 la formation basée sur les rôles et déclenchée par un événement ;

1.4.5 les éléments de preuve d'achèvement de la formation ;

1.4.6 l'escalade en cas de non-achèvement ;

1.4.7 la revue de l'efficacité de la formation ;

1.4.8 les éléments de preuve d'assurance de formation des sous-traitants, des sous-traitants ultérieurs et des tiers.

1.5 La présente politique ne crée pas de matrice de formation, de tableau de bord de formation, de registre des ressources humaines, de registre des compétences, de registre disciplinaire ni de registre de formation des clients distinct. Les affectations de formation, les achèvements, les rappels, les éléments de preuve de compétence et les éléments de preuve de sensibilisation sont enregistrés dans REG11, les exceptions, escalades, non-conformités, actions correctives et éléments de preuve de revue étant enregistrés dans REG12. Les éléments de preuve d'assurance de formation des sous-traitants, des sous-traitants ultérieurs et des tiers sont enregistrés dans REG08 lorsque cela est pertinent.

1.6 La présente politique ne duplique pas :

1.6.1 l'attribution des responsabilités liées aux rôles dans PII02 ;

1.6.2 les exigences relatives à l'inventaire des traitements et à la base légale dans PII03 ;

1.6.3 la méthodologie d'appréciation des risques relatifs à la vie privée et de DPIA dans PII07 ;

1.6.4 les points de contrôle de protection de la vie privée dès la conception dans PII08 ;

1.6.5 la gouvernance du cycle de vie des sous-traitants dans PII12 ;

1.6.6 l'exploitation de la sécurité et du contrôle d'accès des PII dans PII14 ;

1.6.7 le flux de travail relatif aux incidents et violations de PII dans PII15 ;

1.6.8 la gouvernance des informations documentées dans PII17 ;

1.6.9 la gouvernance de la surveillance, de l'audit interne et de l'amélioration dans PII18.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les personnes dont les travaux affectent le traitement des PII comprennent leurs responsabilités en matière de vie privée, suivent une formation appropriée selon une périodicité définie, maintiennent une compétence adaptée à leur rôle et produisent des éléments de preuve auditables de formation, de sensibilisation et d'escalade.

2.2 La présente politique favorise une mise en œuvre cohérente du PIMS en utilisant REG11 comme principal objet d'éléments de preuve pour la formation et la sensibilisation, et REG08, REG10 et REG12 comme objets d'éléments de preuve à l'appui.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir les publics cibles de la formation à la vie privée ;

3.1.2 définir les exigences de formation d'intégration ;

3.1.3 définir les exigences de formation de rappel annuelle ;

3.1.4 définir les exigences de formation à la vie privée basée sur les rôles ;

3.1.5 enregistrer les éléments de preuve d'achèvement dans REG11 ;

3.1.6 faire escalader les non-achèvements au moyen de REG12 ;

3.1.7 conserver les éléments de preuve d'assurance de formation des sous-traitants, des sous-traitants ultérieurs et des tiers dans REG08 lorsque cela est pertinent ;

3.1.8 revoir l'efficacité de la formation sans créer d'indicateurs excessifs ni de registres en double ;

3.1.9 veiller à ce que le contenu de formation reste aligné sur les politiques PIMS en vigueur et les obligations substantielles en matière de vie privée.

4. Énoncés de politique

4.1 Public cible de la formation et affectation

4.1.1 [All] Privacy Lead / PIMS Manager doit définir les catégories de publics cibles de la formation PIMS dans REG11 avant le début de chaque cycle annuel de formation.

4.1.2 [All] Process Owner / Business Owner doit identifier dans REG11 le personnel dont les fonctions impliquent le traitement des PII avant l'intégration, l'attribution du rôle ou toute modification substantielle des fonctions.

4.1.3 [Conditional] System Owner / Application Owner doit identifier dans REG11 les utilisateurs nécessitant une formation à la vie privée relative aux systèmes PII, à l'accès à privilèges ou à l'administration avant que l'accès ne soit activé ou substantiellement modifié.

4.1.4 [Joint Controller] Privacy Lead / PIMS Manager doit enregistrer la répartition des responsabilités de formation entre responsables conjoints du traitement dans REG11 ou REG08 avant que l'activité de traitement conjoint ne commence ou ne soit substantiellement modifiée.

4.1.5 [Conditional] Data Protection Officer / Privacy Advisor doit identifier dans REG11 les besoins renforcés de formation à la vie privée avant que la formation ne soit affectée aux rôles traitant des traitements à haut risque, des PII de catégories particulières, des droits des personnes concernées, des DPIAs, des transferts internationaux ou de l'évaluation d'une violation de données à caractère personnel.

4.1.6 [All] Privacy Lead / PIMS Manager doit enregistrer dans REG11 le public cible de la formation affecté, le type de formation, la date d'achèvement requise et le propriétaire des éléments de preuve avant le début de chaque cycle annuel de formation.

4.2 Périodicité de l'intégration et de la formation annuelle

4.2.1 [All] Privacy Lead / PIMS Manager doit affecter dans REG11 une formation de base de sensibilisation à la vie privée dans un délai de 10 jours ouvrés à compter de l'intégration pour le personnel ayant accès aux PII ou assumant des responsabilités PIMS.

4.2.2 [All] Process Owner / Business Owner doit veiller à ce que le personnel affecté achève la formation d'intégration à la vie privée dans REG11 avant l'approbation de tout accès non

supervisé aux PII ou dans un délai de 30 jours à compter de l'intégration, selon l'échéance la plus proche.

4.2.3 [All] Privacy Lead / PIMS Manager doit affecter dans REG11 une formation de rappel annuelle à la vie privée au moins une fois tous les 12 mois.

4.2.4 [All] Process Owner / Business Owner doit confirmer dans REG11 le statut d'achèvement de la formation de rappel annuelle pour le personnel affecté au plus tard à la date d'échéance annuelle publiée.

4.2.5 [Conditional] Privacy Lead / PIMS Manager doit affecter dans REG11 une formation de rappel ciblée dans un délai de 30 jours après une modification substantielle d'une politique de vie privée, une modification substantielle d'un processus PIMS, un constat d'audit, un échec récurrent de formation ou une leçon pertinente tirée d'un incident PII.

[... 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] Process Owner / Business Owner doit enregistrer dans REG12 une demande d'exception relative à la formation à la vie privée avant toute prolongation d'une échéance d'achèvement requise.

9.1.2 [All] Privacy Lead / PIMS Manager doit approuver ou rejeter les demandes d'exception relatives à la formation à la vie privée dans REG12 avant que l'exception ne devienne active.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor doit conseiller sur les exceptions de formation dans REG12 avant approbation lorsque l'exception affecte un traitement à haut risque, des PII de catégories particulières, la gestion des droits, la gestion des incidents, les transferts internationaux ou les éléments de preuve de certification.

9.1.4 [Conditional] Top Management doit approuver dans REG12 les exceptions relatives à la formation à la vie privée avant leur activation lorsque l'exception affecte un non-achèvement répété, un accès privilégié aux PII, un traitement des PII à fort impact ou des éléments de preuve destinés aux régulateurs.

9.1.5 [All] Privacy Lead / PIMS Manager doit définir dans REG12 le propriétaire de l'exception, la date d'expiration, l'action compensatoire et la date de revue avant d'approuver toute exception relative à la formation à la vie privée.

9.1.6 [All] Process Owner / Business Owner doit clôturer ou renouveler les exceptions approuvées relatives à la formation à la vie privée dans REG12 avant la date d'expiration de l'exception.

10. Application de la politique

10.1.1 [All] Privacy Lead / PIMS Manager doit enregistrer une non-conformité de formation dans REG12 dans un délai de cinq jours ouvrés lorsque les éléments de preuve de formation obligatoire à la vie privée sont manquants, incomplets, en retard ou non traçables à REG11.

10.1.2 [All] Process Owner / Business Owner doit veiller à ce que toute formation obligatoire à la vie privée en retard soit achevée ou fasse l'objet d'une escalade dans REG11 ou REG12 dans un délai de 10 jours ouvrés après l'enregistrement du statut en retard.

10.1.3 [Conditional] System Owner / Application Owner doit restreindre dans REG12 tout nouvel accès aux PII à fort impact lorsque la formation d'intégration ou la formation à la vie privée basée sur les rôles requise demeure incomplète après escalade.

10.1.4 [Processor] Vendor / Procurement Owner doit faire escalader les éléments de preuve d'assurance de formation manquants concernant les sous-traitants, les sous-traitants ultérieurs

ou le personnel externe dans REG08 et REG12 dans un délai de cinq jours ouvrés après leur identification.

10.1.5 [Conditional] Incident Response Coordinator doit lier les mesures d'application liées à la formation à REG10 dans un délai d'un jour ouvré lorsque l'échec de formation a contribué à un incident PII suspecté ou confirmé.

10.1.6 [All] Internal Audit / Compliance Reviewer doit vérifier les éléments de preuve de clôture des actions correctives de formation dans REG12 lors du prochain audit planifié ou dans un délai de 60 jours à compter de la clôture, selon l'échéance la plus proche.

11. Revue et maintenance

11.1.1 [All] Privacy Lead / PIMS Manager doit revoir la présente politique et le contenu de formation au moins une fois par an et enregistrer le résultat de la revue dans REG11 ou REG12.

11.1.2 [All] Privacy Lead / PIMS Manager doit revoir la présente politique dans un délai de 30 jours après toute modification substantielle du domaine d'application du PIMS, de la législation relative à la vie privée, des activités de traitement, du modèle de rôles, des leçons d'incidents, des constats d'audit ou des résultats d'efficacité de la formation.

11.1.3 [Conditional] Data Protection Officer / Privacy Advisor doit examiner dans REG12 les modifications de politique à enjeu significatif pour la vie privée avant approbation.

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

11.1.5 [All] Privacy Lead / PIMS Manager doit mettre à jour le contenu de formation et les éléments de preuve d'affectation dans REG11 dans un délai de 30 jours après une modification substantielle approuvée de la politique.

12. Politiques associées

12.1 La présente politique doit être lue conjointement avec :

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 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 relative à la collecte, à l'utilisation, à la divulgation et au partage des PII ;

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

12.12 PII12 - Politique de gestion de la vie privée applicable aux sous-traitants, sous-traitants ultérieurs et tiers ;

12.13 PII13 - Politique relative aux transferts internationaux de PII ;

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

12.15 PII15 - Politique de gestion des incidents et violations de PII ;

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

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

13. Normes et référentiels de référence

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].