					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII02					Titre du document : **Politique relative aux rôles, responsabilités et à la responsabilité 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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Contexte du rôle PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Leadership et responsabilité
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Rôles, responsabilités et autorités PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Compétence liée aux rôles
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Sensibilisation liée aux rôles
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Communication relative aux rôles
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informations documentées relatives aux rôles
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Propriété du contrôle opérationnel
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Rôle d’audit indépendant
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revue de direction de la responsabilité
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non-conformité et action corrective liées aux rôles
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Responsabilité contractuelle du sous-traitant
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Rôles et responsabilités du responsable conjoint du traitement
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Enregistrements de responsabilité
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Accords clients et instructions applicables au sous-traitant

ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Alignement des finalités du sous-traitant
GDPR	Article 5(2)	Controller	Supporting	Éléments de preuve de responsabilité
GDPR	Article 24	Controller	Supporting	Responsabilité et mesures du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Accords entre responsables conjoints du traitement
GDPR	Article 28	Both	Supporting	Gouvernance du sous-traitant et instructions
GDPR	Article 30	Both	Supporting	Registres des traitements et éléments de preuve de responsabilité
GDPR	Article 37	Conditional	Referenced	Désignation du DPO le cas échéant
GDPR	Article 38	Conditional	Supporting	Position et indépendance du DPO le cas échéant
GDPR	Article 39	Conditional	Supporting	Tâches du DPO le cas échéant
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Acteurs et rôles du cadre de protection de la vie privée
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Responsabilité de la conformité en matière de vie privée
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Rôles de protection des PII et séparation des tâches
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Rôles et responsabilités en sécurité de l’information

ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Séparation des tâches

1. Champ d’application

1.1 La présente politique définit le modèle de rôles PIMS, la structure de responsabilité, les règles d’attribution des responsabilités, les règles de cumul de rôles, les attentes en matière d’escalade et les exigences relatives aux éléments de preuve pour la gouvernance de la Protection des données.

1.2 La présente politique s’applique au personnel, aux fonctions, aux systèmes, aux fournisseurs, aux sous-traitants, aux sous-traitants ultérieurs et aux relations de responsables conjoints du traitement qui participent au traitement de PII relevant du domaine d’application du PIMS, ou l’influencent.

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 nouveaux intitulés de poste organisationnels. Elle définit des rôles PIMS canoniques pouvant être attribués à du personnel ou à des fonctions existants, sous réserve que l’attribution des rôles, la compétence, l’indépendance et les exigences relatives aux conflits d’intérêts soient documentées.

2. Objet

2.1 La présente politique a pour objet de garantir que les responsabilités PIMS sont clairement attribuées, comprises, communiquées, étayées par des éléments de preuve, revues et améliorées.

2.2 La présente politique permet à l’organisation de démontrer sa responsabilité en matière de gouvernance de la Protection des données, de propriété du traitement de PII, de détermination des rôles de responsable du traitement et de sous-traitant, de répartition des responsabilités entre responsables conjoints du traitement, de gestion des instructions données aux sous-traitants, de responsabilité des fournisseurs en matière de vie privée, de revue indépendante et d’escalade fondée sur les rôles.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir les rôles PIMS canoniques utilisés dans l’ensemble des politiques PIMS ;

3.1.2 garantir qu’un rôle responsable est attribué à chaque responsabilité PIMS significative ;

3.1.3 soutenir la responsabilité du responsable du traitement, du responsable conjoint du traitement, du sous-traitant et du sous-traitant ultérieur ;

3.1.4 permettre un cumul pratique des rôles pour les petites et moyennes organisations, tout en maîtrisant les conflits d’intérêts ;

3.1.5 préserver la revue indépendante assurée par Internal Audit / Compliance Reviewer ;

3.1.6 garantir que les attributions de rôles et les changements de rôles sont consignés dans des objets d’éléments de preuve canoniques ;

3.1.7 garantir que les titulaires de rôles PIMS reçoivent les communications et la sensibilisation appropriées ;

3.1.8 garantir que les lacunes, conflits et non-conformités liés aux rôles font l’objet d’une escalade et sont corrigés.

4. Énoncés de politique

4.1 Modèle de rôles PIMS et attribution

4.1.1 [All] Top Management doit approuver le modèle de rôles PIMS canonique dans REG01 avant la mise en œuvre initiale du PIMS, puis annuellement.

4.1.2 [All] Privacy Lead / PIMS Manager doit tenir à jour les attributions nominatives des rôles PIMS dans REG01 avant la mise en œuvre du PIMS et dans les 10 jours ouvrables suivant tout changement de personnel ou d’organisation.

4.1.3 [All] Privacy Lead / PIMS Manager doit documenter le périmètre de responsabilité et le niveau d'autorité de chaque rôle PIMS attribué dans REG01 avant que l'attribution ne prenne effet.

4.1.4 [All] Process Owner / Business Owner doit attribuer un responsable désigné de l'activité de traitement pour chaque activité de traitement de PII dans REG02 avant le début de l'activité de traitement.

4.1.5 [All] System Owner / Application Owner doit documenter le propriétaire responsable du système pour chaque système traitant des PII dans REG02 avant la mise en production du système.

4.1.6 [All] Vendor / Procurement Owner doit documenter le propriétaire de la relation pour chaque relation avec un sous-traitant, un sous-traitant ultérieur, un partage de données avec un tiers ou un responsable conjoint du traitement dans REG08 avant l'intégration ou l'approbation de l'accord.

4.2 Cumul de rôles, séparation des tâches et indépendance

4.2.1 [All] Privacy Lead / PIMS Manager doit documenter chaque cumul de rôles PIMS dans REG01 avant que ce cumul ne prenne effet.

4.2.2 [All] Top Management doit approuver dans REG01, avant attribution, les cumuls de rôles impliquant Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator ou Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer doit documenter son indépendance à l'égard du processus PIMS faisant l'objet de la revue dans REG12 avant le début de chaque audit PIMS ou revue de conformité.

4.2.4 [All] Privacy Lead / PIMS Manager doit consigner les contrôles compensatoires applicables aux conflits inévitables de séparation des tâches dans REG12 avant d'approuver un cumul de rôles.

4.2.5 [All] Data Protection Officer / Privacy Advisor doit consigner dans REG12 toute préoccupation relative à l'indépendance du rôle ou aux conflits d'intérêts dans un délai de cinq jours ouvrables à compter de 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] Process Owner / Business Owner doit demander une exception de responsabilité des rôles dans REG12 avant d'exploiter une activité de traitement de PII sans rôle attribué requis.

9.1.2 [All] Privacy Lead / PIMS Manager doit évaluer l'impact et les mesures d'atténuation de chaque exception de responsabilité des rôles dans REG12 dans les 10 jours ouvrables suivant la demande.

9.1.3 [All] Top Management doit approuver dans REG12 les exceptions de responsabilité des rôles dépassant 30 jours ou affectant un traitement à risque élevé avant que l'exception ne prenne effet.

9.1.4 [All] Privacy Lead / PIMS Manager doit fixer dans REG12 une date d'expiration n'excédant pas 90 jours pour chaque exception de responsabilité des rôles approuvée avant l'approbation.

9.1.5 [All] Privacy Lead / PIMS Manager doit clôturer ou réévaluer chaque exception de responsabilité des rôles dans REG12 dans un délai de cinq jours ouvrables suivant son expiration.

10. Application de la politique

10.1.1 [All] Privacy Lead / PIMS Manager doit consigner les attributions de rôles PIMS manquantes, inexactes ou obsolètes comme non-conformités dans REG12 dans un délai de cinq jours ouvrables à compter de leur identification.

10.1.2 [All] Top Management doit exiger une action corrective dans REG12 dans un délai de 15 jours ouvrables en cas de défaillances de responsabilité répétées ou prolongées.

10.1.3 [All] Process Owner / Business Owner doit empêcher la mise en production de tout traitement de PII nouveau ou modifié lorsque les éléments de preuve requis relatifs aux rôles et à la responsabilité sont absents de REG02 ou REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer doit vérifier l'efficacité des actions correctives relatives aux non-conformités de responsabilité des rôles dans REG12 lors du prochain audit planifié ou dans les 60 jours suivant la clôture, selon la première de ces échéances.

11. Revue et maintenance

11.1.1 [All] Privacy Lead / PIMS Manager doit revoir la présente politique annuellement et dans les 30 jours suivant tout changement significatif du modèle de rôles PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor doit examiner les modifications proposées de la présente politique au regard de leur impact sur les rôles relatifs à la vie privée dans REG12 avant approbation.

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

11.1.4 [All] Privacy Lead / PIMS Manager doit mettre à jour REG01 et REG11 dans les 15 jours ouvrables suivant les modifications approuvées des rôles, responsabilités ou exigences de communication PIMS.

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

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

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

12.6 PII12 - Politique de gestion de la vie privée des sous-traitants, sous-traitants ultérieurs et tiers

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

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

12.9 PII16 - Politique relative à la formation, à la sensibilisation et à la compétence en matière de vie privée

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

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

13. Normes et référentiels de référence

13.1 La présente politique est mappée aux normes et réglementations suivantes. Le mappage 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 4.1** - Mappée à la détermination du contexte des rôles PIMS, à l'applicabilité des rôles de responsable du traitement et de sous-traitant, à la propriété du traitement et aux

enregistrements de responsabilité des relations. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Mappée à l'approbation par Top Management, à la supervision de la responsabilité, à la revue annuelle de direction, aux indicateurs de responsabilité et aux actions correctives relatives aux défaillances de rôles. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Mappée à l'attribution, à la documentation, à la communication et à la maintenance des rôles, responsabilités et autorités PIMS, ainsi qu'à la propriété des systèmes, à la propriété des traitements, à la propriété des relations fournisseurs, à la propriété de l'escalade des incidents et à la responsabilité de la revue indépendante. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Mappée aux éléments de preuve de compétence et de sensibilisation propres aux rôles pour les responsabilités PIMS attribuées. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Mappée à la sensibilisation aux responsabilités PIMS attribuées, aux éléments de preuve d'attestation et au reporting annuel de la sensibilisation aux rôles. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Mappée à la communication des attributions de rôles, des changements de rôles, des escalades et des informations de passation des responsabilités. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Mappée aux informations documentées relatives aux attributions de rôles PIMS, aux périmètres de responsabilité, aux niveaux d'autorité, à la conservation annuelle des éléments de preuve et à la maintenance de la matrice de rôles. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Mappée à la propriété des contrôles opérationnels pour les activités de traitement, les systèmes, les fournisseurs, les sous-traitants, les sous-traitants ultérieurs, les relations de responsables conjoints du traitement et les contrôles de mise en production. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Mappée à l'audit indépendant et à la revue de conformité des éléments de preuve d'attribution des rôles, des éléments de preuve de cumul de rôles, des éléments de preuve d'indépendance, des constats et de la clôture des actions correctives. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Mappée à la revue de direction de l'exhaustivité de l'attribution des rôles PIMS, des conflits de rôles, des exceptions, des indicateurs de responsabilité et des résultats de la revue de responsabilité. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Mappée à l'escalade, à l'enregistrement des non-conformités, aux actions correctives, à la clôture des exceptions et à la vérification de l'efficacité pour les questions de responsabilité des rôles. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Mappée à l'attribution et à la documentation de la responsabilité contractuelle du sous-traitant et de l'escalade des responsabilités des tiers avant l'approbation ou le renouvellement du contrat. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Mappée à la documentation de la répartition des responsabilités entre responsables conjoints du traitement et des éléments de preuve de responsabilité de la relation avant le début du traitement conjoint. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Mappée à la tenue des enregistrements de responsabilité pour la propriété du traitement par le responsable du traitement, la classification des rôles et la propriété des éléments de preuve. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Mappée à la responsabilité relative aux accords clients du sous-traitant, à la propriété des instructions du client et aux éléments de preuve de la relation de sous-traitance. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Mappée à l'alignement des finalités et instructions du sous-traitant au moyen de la propriété des instructions du client et de la vérification des rôles de responsable du traitement et de sous-traitant. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappée aux éléments de preuve de responsabilité pour les attributions de rôles, la propriété des traitements, les revues de rôles, les non-conformités et les constats d'audit. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mappée à la responsabilité du responsable du traitement, à la propriété responsable du traitement, à la supervision par Top Management, à la revue annuelle et aux mesures de responsabilité. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Mappée à la documentation de la répartition des responsabilités entre responsables conjoints du traitement et des éléments de preuve de responsabilité de la relation avant le début du traitement conjoint. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Mappée à la répartition des responsabilités du sous-traitant et du sous-traitant ultérieur, à la propriété des instructions du client, à la responsabilité contractuelle et aux circuits d'escalade des tiers. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Mappée aux registres des traitements, à la propriété des traitements, à la classification des rôles PIMS et à la vérification des rôles de responsable du traitement et de sous-traitant. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Mappée à la documentation du rôle Data Protection Officer / Privacy Advisor lorsque la désignation est applicable ou volontairement attribuée. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Mappée à la position, à l'indépendance, à l'implication et à la gestion des conflits d'intérêts de Data Protection Officer / Privacy Advisor le cas échéant. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Mappée aux conseils relatifs à la vie privée, aux observations de surveillance, à la revue consultative et à la revue de l'impact sur la vie privée liée aux rôles par Data Protection Officer / Privacy Advisor le cas échéant. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Mappée aux acteurs du cadre de protection de la vie privée et à l'allocation des rôles pour les personnes concernées, les responsables du traitement de PII, les sous-traitants de PII, les tiers et la classification des rôles PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Mappée à la responsabilité de la conformité en matière de vie privée, aux éléments de preuve de rôle, aux revues, aux constats d'audit et à la vérification des actions correctives. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Mappée à la définition des rôles de protection des PII, à la documentation des rôles, à la communication des rôles, à la coordination sécurité/vie privée et à la séparation des tâches pour la protection des PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Mappée à la définition, à l'allocation, à la documentation, à la communication et à la maintenance des responsabilités PIMS et de sécurité de l'information. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Mappée à la séparation des tâches, à l'approbation du cumul de rôles, à la revue indépendante, aux contrôles des conflits et à la vérification des actions correctives relatives aux conflits de rôles. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].