					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII09					Titre du document : **Politique relative à la collecte, à l'utilisation, à la divulgation et au partage 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**

Mentions légales (droits d'auteur et restrictions d'utilisation)

(C) 2025 Clarysec LLC. All rights reserved.

Le présent document est la propriété intellectuelle de Clarysec LLC. Aucune partie de ce document ne peut être copiée, réutilisée, distribuée ou modifiée à des fins commerciales ou de mise en œuvre sans autorisation écrite expresse préalable.

Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.

Pour toute demande de licence, contactez : info@clarysec.com

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	Contrôle opérationnel documenté
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance et action corrective
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Finalité et registres de traitement
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Articulation avec la base légale
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Responsabilités de partage entre responsables conjoints du traitement
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
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Articulation avec le routage des transferts
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registres des transferts et des divulgations
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Instructions et registres du sous-traitant
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Articulation avec le routage des transferts par le sous-traitant
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registres des divulgations et demandes du sous-traitant
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Limitation des finalités, minimisation et responsabilité
GDPR	Article 6	Controller	Referenced	Articulation avec la base légale

GDPR	Article 24	Controller	Supporting	Responsabilité du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Accords entre responsables conjoints du traitement
GDPR	Article 28	Both	Supporting	Instructions du sous-traitant et limites de divulgation
GDPR	Article 30	Both	Supporting	Registres de traitement et des destinataires
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Limitation des finalités, de la collecte, de la minimisation et de la divulgation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Responsabilité et conformité relative à la vie privée
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Contrôles relatifs aux finalités, à la collecte, à la minimisation, à l'utilisation et à la divulgation

1. Champ d’application

1.1 La présente politique définit les exigences applicables à la collecte, à l’utilisation, à la divulgation et au partage des PII dans le domaine d’application du PIMS.

1.2 La présente politique s’applique aux éléments suivants :

1.2.1 la collecte de PII par des canaux directs, indirects, automatisés, manuels, internes, externes et tiers ;

1.2.2 l’utilisation interne approuvée de PII par les processus métier, systèmes et applications ;

1.2.3 la réutilisation de PII pour une finalité nouvelle ou substantiellement modifiée ;

1.2.4 la divulgation externe de PII à des destinataires, partenaires, autorités, sous-traitants, sous-traitants ultérieurs, fournisseurs et autres tiers ;

1.2.5 les dispositifs récurrents de partage de données et les divulgations ponctuelles ;

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

1.2.7 REG02 - Inventaire des traitements de PII / ROPA, REG08 - Registre des sous-traitants, des sous-traitants ultérieurs et du partage de données, REG09 - Registre des transferts internationaux, et REG12 - Registre des audits, non-conformités, actions correctives et améliorations.

1.3 La présente politique ne remplace pas :

1.3.1 PII03 pour l’inventaire des traitements, la base légale et la responsabilité du ROPA ;

1.3.2 PII04 pour le contenu, la publication et la gestion des versions des mentions d’information ;

1.3.3 PII05 pour le fonctionnement du consentement et des préférences ;

1.3.4 PII06 pour le traitement des demandes d’exercice des droits des personnes concernées ;

1.3.5 PII07 pour la méthodologie de DPIA et l’appréciation des risques relatifs à la vie privée ;

1.3.6 PII08 pour les points de contrôle de protection de la vie privée dès la conception ;

1.3.7 PII10 pour l’exécution de la conservation, de la suppression et de l’élimination ;

1.3.8 PII11 pour la gestion de l’exactitude et de la qualité ;

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

1.3.10 PII13 pour la sélection des mécanismes de transfert international et les contrôles des risques liés aux transferts ;

1.3.11 PII14 pour la sécurité des PII et le contrôle d’accès ;

1.3.12 PII15 pour la gestion des incidents et des violations ;

1.3.13 PII18 pour la gouvernance à l’échelle du PIMS relative à la surveillance, à l’audit, aux non-conformités, aux actions correctives et à l’amélioration.

1.4 Aux fins de la présente politique :

1.4.1 « utilisation approuvée » désigne une utilisation de PII consignée dans REG02 pour une activité de traitement, une finalité, une catégorie de PII, une catégorie de personne concernée, un responsable métier et un rôle PIMS applicable spécifiques.

1.4.2 « collecte » désigne l’obtention de PII directement auprès d’une personne concernée, indirectement auprès d’une autre partie, automatiquement à partir d’un système ou d’un dispositif, ou au moyen d’une source de données interne ou externe.

1.4.3 « réutilisation » désigne l’utilisation de PII pour une finalité qui n’est pas déjà consignée comme finalité approuvée dans REG02 pour l’activité de traitement concernée.

1.4.4 « test de compatibilité » désigne une évaluation documentée dans REG02 portant sur la finalité initiale, la finalité proposée, la dépendance à la base légale, les catégories de PII, les attentes des personnes concernées, la justification de la minimisation, l'impact de la divulgation ou du transfert, ainsi que le routage vers d'autres politiques PIMS si nécessaire.

1.4.5 « divulgation externe » désigne le fait de mettre des PII à la disposition d'une partie extérieure à l'organisation ou extérieure à la chaîne documentée des instructions du client.

1.4.6 « partage de données » désigne un dispositif récurrent ou structuré dans le cadre duquel des PII sont divulguées, transférées, consultées, échangées ou mises à la disposition d'une autre partie.

1.4.7 « partage récurrent sensible » désigne un partage récurrent portant sur des PII de catégories particulières, des PII relatives à des infractions pénales, des PII d'enfants, des enregistrements à fort impact, un partage à grande échelle, ou un partage externe impliquant un lieu de transfert consigné dans REG09.

2. Objet

2.1 La présente politique a pour objet de veiller à ce que les PII soient collectées, utilisées, divulguées et partagées uniquement pour des finalités documentées, approuvées, limitées et assorties d'une responsabilité.

2.2 La présente politique permet à l'organisation de démontrer que la collecte et l'utilisation sont reliées aux enregistrements de traitement dans REG02, que les divulgations et les dispositifs de partage de données sont consignés dans REG08, que le routage des transferts internationaux est relié à REG09, et que les exceptions et non-conformités sont traitées au moyen de REG12.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 limiter la collecte aux PII nécessaires aux finalités documentées ;

3.1.2 veiller à ce que l'utilisation interne des PII soit approuvée avant le début du traitement ;

3.1.3 exiger des tests de compatibilité avant toute réutilisation ;

3.1.4 exiger une approbation et des éléments de preuve avant toute divulgation externe ;

3.1.5 conserver les éléments de preuve du partage de données dans REG08 sans créer de registre distinct de partage de données ;

3.1.6 router les dépendances relatives aux transferts internationaux vers REG09 et PII13 sans dupliquer les contrôles des mécanismes de transfert ;

3.1.7 définir la périodicité de revue du partage récurrent ;

3.1.8 conserver des éléments de preuve compatibles avec les exigences d'audit pour la collecte, l'utilisation, la divulgation, le partage, les exceptions et les actions correctives.

4. Énoncés de politique

4.1 Limitation de la collecte

4.1.1 [Controller] Le Process Owner / Business Owner doit consigner dans REG02 la finalité de la collecte, la source ou le canal, les catégories de PII, les catégories de personnes concernées et les éléments de données minimaux avant le début de toute nouvelle activité de collecte ou de toute modification substantielle de collecte.

4.1.2 [Controller] Le Privacy Lead / PIMS Manager doit examiner l'enregistrement de collecte dans REG02 avant le début de la collecte lorsqu'une nouvelle catégorie de PII, source, canal ou finalité est ajouté.

4.1.3 [Controller] Le Process Owner / Business Owner doit consigner dans REG02 une justification de nécessité pour chaque élément de données PII avant que cet élément ne soit collecté.

4.1.4 [Processor] Le Process Owner / Business Owner doit consigner dans REG02 la référence d'instruction du client issue de REG08 avant de collecter des PII pour le compte d'un client.

4.1.5 [Joint Controller] Le Process Owner / Business Owner doit consigner dans REG08 la répartition des responsabilités de collecte entre responsables conjoints du traitement avant le début de la collecte conjointe.

4.2 Contrôles relatifs à l'utilisation interne approuvée

4.2.1 [Controller] Le Process Owner / Business Owner doit consigner dans REG02 les règles d'utilisation interne approuvée pour chaque activité de traitement avant le début de l'utilisation.

4.2.2 [Controller] Le System Owner / Application Owner doit mettre en œuvre uniquement les champs de workflow, rapports ou exports d'utilisation interne disposant d'une règle d'utilisation approuvée correspondante dans REG02 avant la mise en production.

4.2.3 [Processor] Le Process Owner / Business Owner doit consigner dans REG08 l'alignement avec les instructions du client avant d'utiliser les PII du client pour toute activité de sous-traitant ou de sous-traitant ultérieur.

4.2.4 [Controller] Le Privacy Lead / PIMS Manager doit examiner les règles d'utilisation approuvée dans REG02 au moins une fois par an pour chaque activité de traitement active.

4.2.5 [All] Le Privacy Lead / PIMS Manager doit consigner une non-conformité dans REG12 dans un délai de cinq jours ouvrables lorsqu'une utilisation interne non documentée de PII est identifiée.

[... 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] Le Process Owner / Business Owner doit consigner une demande d'exception dans REG12 avant de déroger à une règle approuvée de collecte, d'utilisation, de divulgation ou de partage.

9.1.2 [All] Le Privacy Lead / PIMS Manager doit consigner une décision d'approbation ou de rejet dans REG12 avant l'activation d'une exception.

9.1.3 [Conditional] Le Data Protection Officer / Privacy Advisor doit consigner son avis dans REG12 avant l'approbation d'une exception impliquant une réutilisation incompatible, un partage récurrent sensible, un conflit relatif à une divulgation juridiquement contraignante ou un routage de transfert.

9.1.4 [All] Top Management doit consigner son approbation dans REG12 avant l'activation de toute exception d'une durée supérieure à 30 jours calendaires ou affectant plus d'une activité de traitement.

9.1.5 [All] Le Process Owner / Business Owner doit clôturer une exception dans REG12 à la date d'expiration ou dans un délai de cinq jours ouvrables après la fin de la condition justifiant l'exception.

10. Mise en application

10.1.1 [All] Le Privacy Lead / PIMS Manager doit consigner toute collecte, utilisation, divulgation ou tout partage non approuvé comme une non-conformité dans REG12 dans un délai de cinq jours ouvrables après son identification.

10.1.2 [Controller] Le Process Owner / Business Owner doit suspendre la collecte, l'utilisation, la divulgation ou le partage dans un délai d'un jour ouvrable lorsque le Privacy Lead / PIMS

Manager consigne dans REG12 l'absence d'éléments de preuve approuvés dans REG02 ou REG08.

10.1.3 [Processor] Le Process Owner / Business Owner doit consigner une décision d'arrêt ou d'escalade dans REG08 et REG12 dans un délai d'un jour ouvrable lorsque des PII du client sont utilisées ou divulguées en dehors des instructions documentées.

10.1.4 [All] Top Management doit examiner dans REG12 les non-conformités non résolues à fort impact relatives à la collecte, à l'utilisation, à la divulgation ou au partage dans un délai de 30 jours calendaires après escalade.

10.1.5 [All] L'Internal Audit / Compliance Reviewer doit vérifier dans REG12 les éléments de preuve de clôture des actions correctives dans un délai de 15 jours ouvrables après que le Privacy Lead / PIMS Manager a marqué la clôture.

11. Revue et maintenance

11.1.1 [All] Le Privacy Lead / PIMS Manager doit examiner la présente politique au moins une fois par an et consigner la décision dans REG12.

11.1.2 [All] Le Privacy Lead / PIMS Manager doit examiner la présente politique dans un délai de 30 jours calendaires suivant une modification substantielle du domaine d'application du PIMS, des finalités de traitement, du modèle de partage, du routage des transferts ou d'une obligation applicable, et consigner le résultat dans REG12.

11.1.3 [All] Le Process Owner / Business Owner doit recertifier les enregistrements actifs REG02 et REG08 au moins une fois par an et dans un délai de 30 jours calendaires suivant une modification substantielle du traitement.

11.1.4 [All] L'Internal Audit / Compliance Reviewer doit inclure les contrôles PII09 dans l'échantillonnage d'audit annuel et consigner la couverture dans REG12.

11.1.5 [All] Le Privacy Lead / PIMS Manager doit mettre à jour les références aux politiques associées dans REG12 dans un délai de dix jours ouvrables lorsque PII03, PII08, PII10, PII12, PII13, PII14 ou PII18 modifie le périmètre opérationnel de la présente politique.

12. Politiques associées

12.1 La présente politique doit être lue conjointement avec :

12.1.1 PII01 - Politique du système de management des informations relatives à la vie privée

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

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

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

12.1.5 PII05 - Politique de gestion du consentement et des préférences

12.1.6 PII06 - Politique de gestion des droits des personnes concernées

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

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

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

12.1.10 PII11 - Politique relative à l'exactitude et à la qualité des PII

12.1.11 PII12 - Politique de gestion de la vie privée relative aux sous-traitants, sous-traitants ultérieurs et tiers

12.1.12 PII13 - Politique relative aux transferts internationaux de PII

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

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

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

12.1.16 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** - Correspond aux enregistrements opérationnels documentés et à la maîtrise des éléments de preuve relatifs à la collecte, à l'utilisation approuvée, à la réutilisation, à la divulgation, au partage et au routage des transferts. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Correspond à la surveillance, à la mesure, à la revue, à la gestion des exceptions, aux non-conformités et aux actions correctives relatives aux contrôles de collecte, d'utilisation, de divulgation et de partage. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Correspond aux finalités documentées du responsable du traitement, aux enregistrements d'utilisation approuvée et aux éléments de preuve de traitement dans REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Correspond à l'articulation avec la base légale pour la collecte, l'utilisation et le routage de la réutilisation, sans remplacer PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Correspond aux éléments de preuve relatifs à la collecte et aux responsabilités de partage entre responsables conjoints du traitement dans REG08. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Correspond à la limitation de la collecte, à la limitation du traitement et à la justification de la minimisation avant la collecte ou l'utilisation de PII. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Correspond à l'articulation du routage des transferts via REG09, sans remplacer les contrôles des mécanismes de transfert prévus par PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Correspond aux registres des transferts, des divulgations et des dispositifs récurrents de partage de données dans REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Correspond à l'alignement du sous-traitant avec les instructions du client et aux registres du sous-traitant relatifs aux limites de collecte, d'utilisation et de réutilisation. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Correspond à l'articulation du routage des transferts par le sous-traitant via REG09, sans remplacer les contrôles des mécanismes de transfert prévus par PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Correspond aux registres des divulgations du sous-traitant, au statut de notification des demandes de divulgation et aux éléments de preuve d'autorisation de divulgation dans REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Correspond aux éléments de preuve relatifs à la limitation des finalités, à la minimisation des données et à la responsabilité pour la collecte, l'utilisation, la réutilisation, la divulgation et le partage. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Correspond à l'articulation avec la base légale et au routage pour une réutilisation nouvelle ou incompatible, sans remplacer PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Correspond à la gouvernance, aux approbations, à la revue et aux mesures de responsabilité du responsable du traitement pour la collecte, l'utilisation, la divulgation et le partage. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Correspond aux éléments de preuve relatifs à la collecte et aux responsabilités de partage entre responsables conjoints du traitement. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Correspond à l'alignement des instructions des sous-traitants et sous-traitants ultérieurs, à l'autorisation du client et aux limites de divulgation. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Correspond aux registres de traitement, des destinataires, des divulgations et du partage dans REG02 et REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Correspond à la spécification des finalités, à la limitation de la collecte, à la minimisation des données, à la limitation de l'utilisation et à la limitation de la divulgation. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Correspond à la responsabilité, aux éléments de preuve de conformité, à la revue, à la gestion des exceptions, à l'échantillonnage d'audit et aux actions correctives. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Correspond aux finalités, à la limitation de la collecte, à la minimisation, à la limitation de l'utilisation, à la limitation de la divulgation et à l'appui des registres de divulgation. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].