

				Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII03				Titre du document : Politique d'inventaire des traitements PII et de base légale							
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

<p>Mentions légales (droits d'auteur et restrictions d'utilisation) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>Toute utilisation non autorisée est strictement interdite et peut entraîner des poursuites judiciaires.</p> <p>Pour toute demande de licence, contactez : info@clarysec.com</p>

Alignement sur les normes et réglementations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Supporting	Détermination du rôle PIMS pour les activités de traitement
ISO/IEC 27701:2025	Clause 6.1.2	Both	Supporting	Lien avec les déclencheurs de l'appréciation des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Lien avec l'applicabilité des contrôles et la SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informations documentées relatives à l'inventaire des traitements
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Planification et maîtrise opérationnelles des enregistrements de traitement
ISO/IEC 27701:2025	Clause 8.2	Both	Supporting	Lien avec l'appréciation opérationnelle des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Surveillance et mesure de l'inventaire
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non-conformité de l'inventaire et action corrective
ISO/IEC 27701:2025	Annex A.1.2.2	Controller	Primary	Identification des finalités par le responsable du traitement
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Primary	Identification de la base légale par le responsable du traitement
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Supporting	Lien avec l'examen préalable DPIA

ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Enregistrements des responsabilités de traitement des responsables conjoints du traitement
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Enregistrements du responsable du traitement relatifs au traitement PII
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Enregistrements des accords clients et des instructions du sous-traitant
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Primary	Alignement des finalités du sous-traitant sur les instructions du client
ISO/IEC 27701:2025	Annex A.2.2.7	Processor	Supporting	Enregistrements du sous-traitant relatifs au traitement PII
GDPR	Article 5(1)(a)	Controller	Supporting	Lien avec la licéité, la loyauté et la transparence
GDPR	Article 5(1)(b)	Controller	Supporting	Limitation des finalités
GDPR	Article 5(1)(c)	Controller	Supporting	Minimisation des données
GDPR	Article 5(1)(e)	Controller	Supporting	Lien avec la limitation de la conservation
GDPR	Article 5(2)	Controller	Supporting	Éléments de preuve de responsabilité
GDPR	Article 6	Controller	Primary	Licéité du traitement
GDPR	Article 9	Conditional	Supporting	Condition applicable au traitement de catégories particulières
GDPR	Article 10	Conditional	Supporting	Condition applicable aux données relatives aux condamnations

				pénales et aux infractions
GDPR	Article 24	Controller	Supporting	Responsabilité et mesures du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Enregistrements des accords entre responsables conjoints du traitement
GDPR	Article 28	Both	Supporting	Enregistrements des instructions et des accords du sous-traitant
GDPR	Article 30	Both	Primary	Registres des activités de traitement
GDPR	Article 35	Controller	Supporting	Lien avec l'examen préalable DPIA
ISO/IEC 29100:2020	Clause 5.3	Both	Supporting	Légitimité et spécification des finalités
ISO/IEC 29100:2020	Clause 5.4	Both	Supporting	Limitation de la collecte
ISO/IEC 29100:2020	Clause 5.5	Both	Supporting	Minimisation des données
ISO/IEC 29100:2020	Clause 5.6	Both	Supporting	Limitation de l'utilisation, de la conservation et de la divulgation
ISO/IEC 29100:2020	Clause 5.10	Both	Supporting	Responsabilité
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Controller	Supporting	Contrôles de protection PII relatifs aux finalités, à la collecte, à la minimisation, à l'utilisation, à la conservation et à la divulgation
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Both	Supporting	Lien avec les bénéfices et les déclencheurs de la PIA

1. Champ d'application

1.1 La présente politique définit les exigences relatives à la tenue de l'inventaire des traitements PII / ROPA et à la documentation de la base légale, des finalités de traitement, des rôles de traitement, des catégories de PII, des catégories de personnes concernées, des destinataires, des références de conservation, des références de transfert, des instructions des sous-traitants, des enregistrements de responsables conjoints du traitement et du lien avec l'examen préalable des risques relatifs à la vie privée.

1.2 La présente politique s'applique :

- 1.2.1 à toutes les activités de traitement PII relevant du domaine d'application du PIMS ;
- 1.2.2 aux traitements réalisés en qualité de responsable du traitement, de responsable conjoint du traitement, de sous-traitant ou de sous-traitant ultérieur ;
- 1.2.3 aux traitements réalisés par des processus métier, systèmes, applications, fournisseurs, sous-traitants, sous-traitants ultérieurs et destinataires de partage de données ;
- 1.2.4 aux nouveaux traitements, aux traitements ayant fait l'objet d'une modification substantielle et aux traitements retirés ;
- 1.2.5 aux éléments de preuve conservés dans REG02 et aux éléments de preuve à l'appui dans REG01, REG03, REG04, REG05, REG07, REG08, REG09 et REG12.

1.3 La présente politique ne remplace pas les contrôles détaillés relatifs aux mentions d'information sur la vie privée, au consentement, à la méthodologie DPIA, à l'exécution de la conservation, à la sélection des mécanismes de transfert international, aux contrôles contractuels des sous-traitants, aux contrôles de sécurité PII ou aux contrôles des informations documentées. Ces exigences sont définies dans les politiques associées énumérées à la Section 12.

1.4 Aux fins de la présente politique, un enregistrement d'inventaire des traitements désigne une entrée REG02 décrivant une activité distincte de traitement PII, notamment sa finalité, son rôle, son propriétaire, les catégories de PII, les catégories de personnes concernées, la base légale ou la référence d'instruction du client, les systèmes, les destinataires, la référence de conservation, la référence de transfert, le statut de risque relatif à la vie privée et le statut de revue.

1.5 Aux fins de la présente politique, une modification substantielle du traitement désigne toute modification de la finalité du traitement, de la base légale, du rôle PIMS, de la catégorie de PII, de la catégorie de personnes concernées, du destinataire, du système, du fournisseur, du sous-traitant ultérieur, du lieu de traitement, du transfert, de la règle de conservation, de la classification de sécurité, de la mention d'information sur la vie privée, de la dépendance au consentement, du statut DPIA, de l'instruction du client ou du périmètre de certification.

2. Objet

2.1 La présente politique a pour objet de permettre à l'organisation d'identifier, de documenter, de justifier, de revoir et de démontrer les activités de traitement PII relevant du domaine d'application du PIMS.

2.2 La présente politique permet à l'organisation de tenir un inventaire des traitements PII complet, à jour et compatible avec les exigences d'audit, qui soutient le traitement licite, la responsabilité, les mentions d'information sur la vie privée, la gestion du consentement, l'appréciation des risques relatifs à la vie privée, l'examen préalable DPIA, la conservation, la gouvernance des transferts, la gouvernance des sous-traitants et la surveillance du PIMS.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

- 3.1.1 établir REG02 comme l'objet de preuve faisant autorité pour l'inventaire des traitements PII et le ROPA ;

- 3.1.2 s'assurer que chaque activité de traitement PII dispose d'un propriétaire responsable ;
- 3.1.3 distinguer les enregistrements de traitement en qualité de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur ;
- 3.1.4 documenter les finalités spécifiques du traitement avant le début du traitement ;
- 3.1.5 documenter la base légale du traitement réalisé en qualité de responsable du traitement avant le début du traitement ;
- 3.1.6 documenter les instructions du client pour les traitements réalisés en qualité de sous-traitant et de sous-traitant ultérieur avant le début du traitement ;
- 3.1.7 documenter les catégories de PII, les catégories de personnes concernées, les destinataires, les références de conservation, les références de transfert, les systèmes et les relations avec les fournisseurs ;
- 3.1.8 relier les enregistrements d'inventaire aux éléments de preuve relatifs aux mentions d'information sur la vie privée, au consentement, à la DPIA, aux risques, aux fournisseurs, aux transferts, aux contrôles et aux audits, le cas échéant ;
- 3.1.9 s'assurer que les enregistrements d'inventaire des traitements sont revus, mis à jour et corrigés lorsque les traitements changent ;
- 3.1.10 éviter la création de registres distincts de bases légales ou d'inventaires des traitements en dehors de REG02.

4. Énoncés de politique

4.1 Référentiel de base de l'inventaire des traitements

- 4.1.1 [Both] The Process Owner / Business Owner MUST créer un enregistrement d'inventaire des traitements REG02 avant le début de toute nouvelle activité de traitement PII.
- 4.1.2 [Both] The Process Owner / Business Owner MUST renseigner les champs REG02 requis pour chaque activité de traitement avant le début de l'activité.
- 4.1.3 [Both] The Privacy Lead / PIMS Manager MUST approuver l'ensemble des champs REG02 requis dans REG12 avant la mise en service initiale du PIMS, puis annuellement.
- 4.1.4 [Both] The Process Owner / Business Owner MUST classer le rôle PIMS de l'organisation pour chaque activité de traitement dans REG02 avant le début de l'activité.
- 4.1.5 [Both] The System Owner / Application Owner MUST relier chaque système ou application traitant des PII à l'activité de traitement REG02 pertinente avant la mise en production du système.
- 4.1.6 [Both] The Vendor / Procurement Owner MUST relier chaque relation de sous-traitant, de sous-traitant ultérieur, de partage avec un tiers ou de responsable conjoint du traitement figurant dans REG08 à l'activité de traitement REG02 pertinente avant l'approbation de l'accord ou l'intégration.

4.2 Enregistrements des finalités et des bases légales du responsable du traitement

- 4.2.1 [Controller] The Process Owner / Business Owner MUST documenter la finalité spécifique du traitement dans REG02 avant que les PII soient collectées, utilisées, divulguées ou autrement traitées.
- 4.2.2 [Controller] The Privacy Lead / PIMS Manager MUST valider la base légale enregistrée dans REG02 avant le début du traitement en qualité de responsable du traitement et avant toute prise d'effet d'un changement de finalité.
- 4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST consigner son avis dans REG12 avant l'approbation d'une nouvelle base légale pour un traitement à haut risque, des PII de catégories particulières, des données relatives aux condamnations pénales ou aux

infractions, ou un traitement substantiellement modifié réalisé en qualité de responsable du traitement.

- 4.2.4 [Controller] The Process Owner / Business Owner MUST relier REG02 à REG05 avant que le traitement en qualité de responsable du traitement repose sur le consentement comme base légale.
- 4.2.5 [Controller] The Process Owner / Business Owner MUST enregistrer la référence de l'évaluation de l'intérêt légitime dans REG04 avant que le traitement en qualité de responsable du traitement repose sur les intérêts légitimes.
- 4.2.6 [Conditional] The Process Owner / Business Owner MUST enregistrer la condition applicable au traitement de catégories particulières dans REG02 avant de traiter des PII de catégories particulières.
- 4.2.7 [Conditional] The Privacy Lead / PIMS Manager MUST enregistrer la base d'autorisation des données relatives aux condamnations pénales ou aux infractions dans REG02 avant de traiter ces données.
- 4.2.8 [Controller] The Process Owner / Business Owner MUST documenter la compatibilité des finalités et l'examen préalable des risques relatifs à la vie privée dans REG02 et REG04 avant d'utiliser des PII pour une nouvelle finalité non précédemment enregistrée.

[... 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 Exceptions relatives à l'inventaire des traitements et à la base légale

- 9.1.1 [All] The Process Owner / Business Owner MUST demander une exception dans REG12 avant d'exploiter une activité de traitement PII dépourvue d'un champ REG02 requis, d'un enregistrement de base légale, d'une référence d'instruction du client ou d'un statut de revue.
- 9.1.2 [All] The Privacy Lead / PIMS Manager MUST évaluer dans REG12 l'impact sur la vie privée, la certification et les opérations de chaque exception relative à l'inventaire des traitements dans les 10 jours ouvrables suivant la demande.
- 9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST consigner un avis dans REG12 avant l'approbation de toute exception impliquant une base légale, des PII de catégories particulières, des données relatives aux condamnations pénales ou aux infractions, un traitement à haut risque, un lien avec un transfert international ou une limitation liée aux instructions du client.
- 9.1.4 [All] Top Management MUST approuver dans REG12 les exceptions relatives à l'inventaire des traitements dépassant 30 jours, affectant un traitement à haut risque ou affectant le périmètre de certification avant leur prise d'effet.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUST fixer dans REG12 une date d'expiration ne dépassant pas 90 jours pour chaque exception approuvée relative à l'inventaire des traitements avant son approbation.
- 9.1.6 [All] The Process Owner / Business Owner MUST clôturer ou réévaluer chaque exception relative à l'inventaire des traitements dans REG12 dans les cinq jours ouvrables suivant son expiration.

10. Application de la politique

10.1 Application relative à l'inventaire des traitements et à la base légale

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST enregistrer dans REG12 comme non-conformité les éléments de preuve REG02 d'inventaire des traitements manquants, inexacts, obsolètes ou non approuvés dans les cinq jours ouvrables suivant leur identification.

- 10.1.2 [Controller] The Process Owner / Business Owner MUST suspendre tout nouveau traitement en qualité de responsable du traitement lorsque les éléments de preuve requis relatifs à la finalité ou à la base légale sont absents de REG02 avant le lancement.
- 10.1.3 [Processor] The Process Owner / Business Owner MUST suspendre tout nouveau traitement en qualité de sous-traitant lorsque les éléments de preuve requis relatifs aux instructions du client sont absents de REG02 ou REG08 avant l'intégration du service.
- 10.1.4 [Both] The System Owner / Application Owner MUST bloquer la mise en production d'un système pour le traitement PII lorsque le lien d'inventaire REG02 requis est manquant avant l'approbation de la mise en production.
- 10.1.5 [Both] The Vendor / Procurement Owner MUST bloquer l'intégration d'un fournisseur, sous-traitant, sous-traitant ultérieur, destinataire tiers ou responsable conjoint du traitement lorsque les éléments de preuve requis de lien REG02 et REG08 sont manquants avant l'approbation de l'accord.
- 10.1.6 [All] Top Management MUST revoir dans REG12 les non-conformités majeures non résolues relatives à l'inventaire des traitements ou à la base légale lors de la revue de direction.
- 10.1.7 [All] The Internal Audit / Compliance Reviewer MUST vérifier l'efficacité des actions correctives relatives aux non-conformités de l'inventaire des traitements dans REG12 lors du prochain audit planifié ou dans les 60 jours suivant la clôture, selon la première échéance.

11. Revue et maintenance

11.1 Revue et maintenance de la politique

- 11.1.1 [All] The Privacy Lead / PIMS Manager MUST revoir la présente politique dans REG12 annuellement et dans les 30 jours suivant tout changement substantiel des exigences relatives à l'inventaire des traitements, à la base légale, aux instructions des sous-traitants, au ROPA ou à la certification.
- 11.1.2 [All] The Privacy Lead / PIMS Manager MUST revoir les exigences minimales de champs REG02 dans REG12 annuellement et dans les 30 jours suivant tout changement substantiel juridique, réglementaire, contractuel ou de traitement.
- 11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST revoir dans REG12 les changements significatifs pour la vie privée apportés à la présente politique avant approbation.
- 11.1.4 [All] Top Management MUST approuver dans REG12 les changements substantiels apportés à la présente politique avant publication.
- 11.1.5 [All] The Privacy Lead / PIMS Manager MUST mettre à jour REG03 et REG04 dans les 15 jours ouvrables suivant les changements approuvés de la politique qui modifient l'applicabilité des contrôles ou les exigences d'examen préalable des risques relatifs à la vie privée.
- 11.1.6 [All] The Privacy Lead / PIMS Manager MUST enregistrer dans REG11 la communication des changements approuvés de la présente politique 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 du système de management des informations relatives à la vie privée
- 12.3 PII02 - Politique relative aux rôles, responsabilités et responsabilité en matière de vie privée
- 12.4 PII04 - Politique relative aux mentions d'information sur la vie privée et à la transparence
- 12.5 PII05 - Politique de gestion du consentement et des préférences
- 12.6 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA
- 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 PII10 - Politique relative à la conservation, à la suppression et à l'élimination des PII
- 12.10 PII11 - Politique relative à l'exactitude et à la qualité des PII
- 12.11 PII12 - Politique de gestion de la vie privée des sous-traitants, sous-traitants ultérieurs et tiers
- 12.12 PII13 - Politique relative aux transferts internationaux de PII
- 12.13 PII14 - Politique de sécurité PII et de contrôle d'accès
- 12.14 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS
- 12.15 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. La cartographie 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** - Mis en correspondance avec la détermination du rôle PIMS de l'organisation pour chaque activité de traitement et avec la distinction des contextes de responsable du traitement, de responsable conjoint du traitement, de sous-traitant et de sous-traitant ultérieur. Addressed by clauses [4.1.4; 4.3.1; 4.3.4; 4.3.5].
- 13.2.2 **Clause 6.1.2** - Mis en correspondance avec le lien vers les déclencheurs d'appréciation des risques relatifs à la vie privée pour les activités de traitement PII nouvelles et substantiellement modifiées. Addressed by clauses [4.2.8; 4.5.2; 4.5.3].
- 13.2.3 **Clause 6.1.3** - Mis en correspondance avec le rattachement des activités de traitement à l'applicabilité des contrôles et aux éléments de preuve de la Déclaration d'applicabilité du PIMS. Addressed by clauses [4.5.4; 7.1.5; 11.1.5].
- 13.2.4 **Clause 7.5** - Mis en correspondance avec la tenue des enregistrements d'inventaire des traitements, de base légale, d'instructions des sous-traitants, de revue, d'exception et d'action corrective en tant qu'informations documentées maîtrisées. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.2; 4.3.1; 4.4.1; 4.5.1; 7.1.1; 7.1.3; 9.1.1; 10.1.1].
- 13.2.5 **Clause 8.1** - Mis en correspondance avec la planification et la maîtrise opérationnelles de la création, de la validation, de la mise à jour, de la revue et du retrait des enregistrements d'inventaire des traitements avant le début ou le changement du traitement. Addressed by clauses [4.1.1; 4.1.5; 4.1.6; 4.5.1; 4.5.6; 7.1.2; 7.1.6; 7.1.7; 7.1.8].
- 13.2.6 **Clause 8.2** - Mis en correspondance avec le lien de l'appréciation opérationnelle des risques relatifs à la vie privée à partir des enregistrements d'inventaire des traitements et des déclencheurs de modification substantielle du traitement. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].
- 13.2.7 **Clause 9.1** - Mis en correspondance avec la surveillance et la mesure de l'exhaustivité de l'inventaire des traitements, de la validation de la base légale, du lien avec les instructions, du statut de revue, du lien avec l'examen préalable DPIA et des exceptions de rapprochement. Addressed by clauses [4.5.4; 4.5.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].
- 13.2.8 **Clause 10.2** - Mis en correspondance avec le traitement des non-conformités, exceptions, actions correctives, mesures d'application et vérifications d'efficacité relatives à l'inventaire et à la base légale. Addressed by clauses [9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.6; 10.1.7].

- 13.2.9 **Annex A.1.2.2** - Mis en correspondance avec l'identification et la documentation des finalités de traitement du responsable du traitement avant que les PII soient collectées, utilisées, divulguées ou autrement traitées. Addressed by clauses [4.1.2; 4.2.1; 4.2.8; 4.3.5].
- 13.2.10 **Annex A.1.2.3** - Mis en correspondance avec la détermination, la documentation, la validation et la démonstration de la base légale des traitements réalisés en qualité de responsable du traitement. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7].
- 13.2.11 **Annex A.1.2.6** - Mis en correspondance avec l'examen préalable de la nécessité d'une DPIA pour les activités de traitement nouvelles et substantiellement modifiées réalisées en qualité de responsable du traitement. Addressed by clauses [4.5.2; 4.5.3; 8.1.5].
- 13.2.12 **Annex A.1.2.8** - Mis en correspondance avec l'enregistrement des finalités de traitement en responsabilité conjointe et des références de répartition des responsabilités. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.2.13 **Annex A.1.2.9** - Mis en correspondance avec la tenue des enregistrements du responsable du traitement relatifs au traitement PII, notamment les finalités, catégories, destinataires, références de conservation, transferts, bases légales, examen préalable des risques, propriétaire, statut et éléments de preuve de revue. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.4.6; 4.5.1; 4.5.6; 7.1.2; 7.1.8].
- 13.2.14 **Annex A.2.2.2** - Mis en correspondance avec l'accord client du sous-traitant et les éléments de preuve des instructions documentées, notamment l'objet, la durée, la finalité, les catégories de PII et les catégories de personnes concernées. Addressed by clauses [4.3.1; 4.3.2; 5.1.7; 10.1.3].
- 13.2.15 **Annex A.2.2.3** - Mis en correspondance avec l'obligation de veiller à ce que les finalités de traitement du sous-traitant restent alignées sur les instructions documentées du client. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 10.1.3].
- 13.2.16 **Annex A.2.2.7** - Mis en correspondance avec la tenue par le sous-traitant des enregistrements relatifs au traitement de PII pour le compte des clients. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 8.1.3].

13.3 **GDPR**

- 13.3.1 **Article 5(1)(a)** - Mis en correspondance avec la finalité du traitement réalisé en qualité de responsable du traitement, la validation de la base légale et les éléments de preuve de responsabilité avant le début du traitement. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.8].
- 13.3.2 **Article 5(1)(b)** - Mis en correspondance avec la spécification des finalités, l'évaluation de la compatibilité des finalités et la prévention des traitements pour de nouvelles finalités non documentées. Addressed by clauses [4.2.1; 4.2.8; 4.3.3].
- 13.3.3 **Article 5(1)(c)** - Mis en correspondance avec l'enregistrement des catégories de PII, des catégories de personnes concernées et des données sources avant le traitement afin de soutenir la revue de minimisation. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.3.4 **Article 5(1)(e)** - Mis en correspondance avec l'enregistrement de la règle de conservation ou de la référence de conservation pour chaque activité de traitement. Addressed by clauses [4.4.4; 8.1.6].
- 13.3.5 **Article 5(2)** - Mis en correspondance avec les éléments de preuve de responsabilité relatifs à l'inventaire des traitements, à la validation de la base légale, à la revue, au rapprochement, à l'échantillonnage d'audit et aux actions correctives. Addressed by clauses [4.1.1; 4.2.2; 4.5.4; 4.5.5; 6.1.2; 10.1.1; 10.1.7].
- 13.3.6 **Article 6** - Mis en correspondance avec la documentation et la validation de la base légale des traitements réalisés en qualité de responsable du traitement, notamment le lien avec le

- consentement, la référence d'évaluation de l'intérêt légitime et la compatibilité des finalités. Addressed by clauses [4.2.2; 4.2.4; 4.2.5; 4.2.8].
- 13.3.7 Article 9 - Mis en correspondance avec l'enregistrement de la condition applicable au traitement de catégories particulières et de l'avis de protection des données avant le traitement de PII de catégories particulières. Addressed by clauses [4.2.3; 4.2.6; 9.1.3].
- 13.3.8 **Article 10** - Mis en correspondance avec l'enregistrement de la base d'autorisation des données relatives aux condamnations pénales ou aux infractions avant le traitement. Addressed by clauses [4.2.3; 4.2.7; 9.1.3].
- 13.3.9 **Article 24** - Mis en correspondance avec la gouvernance, la revue, la responsabilité et la supervision par la direction des enregistrements d'inventaire des traitements et de base légale du responsable du traitement. Addressed by clauses [4.2.2; 5.1.1; 6.1.2; 10.1.6; 11.1.4].
- 13.3.10 **Article 26** - Mis en correspondance avec les éléments de preuve relatifs à la finalité de traitement en responsabilité conjointe et à la répartition des responsabilités. Addressed by clauses [4.1.6; 4.3.5; 10.1.5].
- 13.3.11 **Article 28** - Mis en correspondance avec les instructions, accords, liens entre les relations et contrôles d'intégration des sous-traitants et sous-traitants ultérieurs. Addressed by clauses [4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 5.1.7; 7.1.7; 10.1.3; 10.1.5].
- 13.3.12 **Article 30** - Mis en correspondance avec les registres des activités de traitement des responsables du traitement et des sous-traitants, notamment les finalités de traitement, les catégories de PII, les catégories de personnes concernées, les destinataires, les transferts, les références de conservation et les enregistrements des instructions du client. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.3.1; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.6; 7.1.2].
- 13.3.13 **Article 35** - Mis en correspondance avec le lien de l'examen préalable DPIA pour les activités de traitement nouvelles, substantiellement modifiées ou à haut risque réalisées en qualité de responsable du traitement. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.3** - Mis en correspondance avec la légitimité des finalités, la spécification des finalités, le lien avec la base légale et les éléments de preuve de compatibilité des finalités. Addressed by clauses [4.2.1; 4.2.2; 4.2.8; 4.3.1; 4.3.3].
- 13.4.2 **Clause 5.4** - Mis en correspondance avec la limitation de la collecte par la documentation des catégories de PII, des catégories de personnes concernées, des sources et de la justification avant le début du traitement. Addressed by clauses [4.1.2; 4.4.1; 4.4.6].
- 13.4.3 **Clause 5.5** - Mis en correspondance avec la minimisation des données au moyen des exigences relatives aux champs de l'inventaire, de la documentation des catégories, de la documentation des destinataires et de la revue des enregistrements de traitement actuels. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.5.4; 8.1.6].
- 13.4.4 **Clause 5.6** - Mis en correspondance avec la limitation de l'utilisation, de la conservation, de la divulgation et des transferts au moyen de finalités documentées, de catégories de destinataires, de références de conservation, du lien avec les transferts et de contrôles des changements de finalité. Addressed by clauses [4.2.1; 4.2.8; 4.4.2; 4.4.4; 4.4.5].
- 13.4.5 **Clause 5.10** - Mis en correspondance avec la responsabilité au moyen de la propriété, de la gouvernance de l'inventaire, de la revue, du rapprochement, de l'échantillonnage d'audit, de la gestion des exceptions et des éléments de preuve d'actions correctives. Addressed by clauses [4.1.1; 4.1.3; 4.5.4; 4.5.5; 5.1.5; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mis en correspondance avec les contrôles de protection PII relatifs à la légitimité des finalités, à la limitation de la collecte, à la minimisation des données et à la limitation de l'utilisation, de la conservation et de la divulgation. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.4; 4.4.6; 4.5.4; 8.1.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Mis en correspondance avec l'utilisation des changements de l'inventaire des traitements pour déclencher l'appréciation des risques relatifs à la vie privée et l'examen préalable DPIA avant la poursuite d'un traitement nouveau ou substantiellement modifié. Addressed by clauses [4.2.8; 4.5.2; 4.5.3; 8.1.5].