					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII07					Titre du document : **Politique d'appréciation des risques relatifs à la vie privée et de DPIA**							
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 6.1.1	Both	Primary	Risques et opportunités du PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Appréciation des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Traitement des risques relatifs à la vie privée et articulation avec la SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Changements planifiés du PIMS et réappréciation des risques
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informations documentées relatives aux risques pour la vie privée et aux DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Planification et maîtrise opérationnelles
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Appréciation opérationnelle des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Traitement opérationnel des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Surveillance et mesure des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revue de direction des risques relatifs à la vie privée
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Non-conformité liée aux risques et action corrective

ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Analyse d'impact relative à la vie privée
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registres des traitements à l'appui de l'appréciation des risques
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Accord client du sous-traitant et assistance à la DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informations du sous-traitant à l'appui de la conformité du client
GDPR	Article 5(2)	Controller	Supporting	Éléments de preuve de responsabilité
GDPR	Article 24	Controller	Supporting	Responsabilité du responsable du traitement et mesures
GDPR	Article 25	Controller	Supporting	Protection des données dès la conception et par défaut
GDPR	Article 28	Both	Supporting	Assistance du sous-traitant et instructions
GDPR	Article 30	Both	Supporting	Registres des traitements à l'appui de la DPIA
GDPR	Article 32	Both	Supporting	Risque de sécurité et mesures de protection
GDPR	Article 35	Controller	Primary	Analyse d'impact relative à la protection des données
GDPR	Article 36	Controller	Primary	Consultation préalable
GDPR	Article 39	Conditional	Supporting	Conseils et surveillance du DPO lorsque applicable

ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Contrôles relatifs à la vie privée, sécurité de l'information et conformité en matière de vie privée
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Périmètre, bénéfices, déclencheur et préparation de la PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Programme de protection des PII et identification des exigences
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Intégration de la gestion organisationnelle des risques relatifs à la vie privée

1. Champ d'application

1.1 La présente politique définit les exigences applicables à l'appréciation des risques relatifs à la vie privée, à l'examen préalable à la DPIA, à la réalisation d'une DPIA complète, au traitement des risques, à l'acceptation du risque résiduel, à la consultation, à la revue et à la gestion des éléments de preuve pour le traitement de PII dans le domaine d'application du PIMS.

1.2 La présente politique s'applique :

1.2.1 aux activités de traitement de PII nouvelles ou substantiellement modifiées ;

1.2.2 aux contextes de traitement en tant que responsable du traitement, responsable conjoint du traitement, sous-traitant et sous-traitant ultérieur ;

1.2.3 aux systèmes, applications, services, processus opérationnels, fournisseurs, sous-traitants, sous-traitants ultérieurs, transferts internationaux et accords de partage de données qui affectent le traitement de PII ;

1.2.4 aux éléments de preuve relatifs aux risques pour la vie privée et aux DPIA conservés dans REG04, ainsi qu'aux éléments de preuve d'appui conservés dans REG02, REG03, REG08, REG09, REG10, REG11 et REG12.

1.3 La présente politique ne remplace pas les contrôles relatifs à l'inventaire des traitements, aux mentions d'information, au consentement, aux droits des personnes concernées, à la protection de la vie privée dès la conception, aux fournisseurs, aux transferts internationaux, à la sécurité des PII, aux incidents, aux informations documentées, ni à la surveillance, à l'audit et à l'amélioration. Ces exigences sont définies dans les politiques associées énumérées à la Section 12.

1.4 Aux fins de la présente politique, l'appréciation des risques relatifs à la vie privée désigne l'identification, l'analyse, l'évaluation, le traitement, la revue et la surveillance documentés des impacts négatifs potentiels sur la vie privée découlant du traitement de PII.

1.5 Aux fins de la présente politique, une DPIA désigne une évaluation documentée utilisée pour un traitement réalisé par un responsable du traitement, susceptible d'engendrer un risque élevé pour les personnes concernées, et qui évalue la nécessité du traitement, sa proportionnalité, les risques, les mesures de protection, le risque résiduel, les besoins de consultation et les conditions d'approbation.

1.6 Aux fins de la présente politique, un risque résiduel élevé relatif à la vie privée désigne un risque pour la vie privée qui demeure supérieur au seuil d'acceptation approuvé après le traitement des risques proposé ou mis en œuvre.

1.7 Aux fins de la présente politique, un changement substantiel désigne tout changement affectant le domaine d'application du PIMS, la finalité du traitement, la base légale, les catégories de PII, les catégories de personnes concernées, l'échelle du traitement, la technologie de traitement, la surveillance ou le profilage, la prise de décision individuelle automatisée, les personnes concernées vulnérables, les destinataires, les sous-traitants, les sous-traitants ultérieurs, les transferts internationaux, la conservation, les contrôles de sécurité, le profil de risque, les instructions du client ou le périmètre de certification.

2. Objet

2.1 La présente politique a pour objet de garantir que les risques relatifs à la vie privée et les obligations de DPIA sont identifiés, évalués, traités, approuvés, revus et étayés avant que le traitement de PII ne crée un risque inacceptable pour les personnes concernées ou pour le PIMS.

2.2 La présente politique permet à l'organisation de démontrer une gouvernance de la Protection des données fondée sur les risques, la responsabilité du responsable du traitement en matière de DPIA, l'assistance du sous-traitant à la DPIA, le traitement documenté des risques, l'approbation du risque résiduel, la prise de décision relative à la consultation préalable et l'amélioration continue des contrôles relatifs à la vie privée.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir les déclencheurs obligatoires de l'examen préalable des risques relatifs à la vie privée ;

3.1.2 définir les cas dans lesquels une DPIA complète est requise ;

3.1.3 veiller à ce que les décisions du responsable du traitement relatives aux DPIA soient documentées et puissent être revues ;

3.1.4 veiller à ce que l'assistance du sous-traitant et du sous-traitant ultérieur à la DPIA soit documentée lorsque l'instruction du client ou l'accord l'exige ;

3.1.5 veiller à ce que les risques relatifs à la vie privée soient appréciés avant la poursuite d'un traitement de PII nouveau ou substantiellement modifié ;

3.1.6 veiller à ce que les traitements des risques relatifs à la vie privée soient attribués, mis en œuvre et vérifiés ;

3.1.7 veiller à ce que les risques résiduels élevés relatifs à la vie privée soient escaladés et approuvés avant le démarrage ou la poursuite du traitement ;

3.1.8 veiller à ce que les décisions de consultation préalable soient documentées lorsqu'un risque résiduel élevé subsiste ;

3.1.9 veiller à ce que les éléments de preuve relatifs aux risques pour la vie privée et aux DPIA soient conservés dans REG04 et liés aux objets de preuve connexes ;

3.1.10 éviter la création de registres distincts de DPIA, de risques ou de consultation en dehors de REG04.

4. Énoncés de politique

4.1 Examen préalable des risques relatifs à la vie privée

4.1.1 [Both] Le Process Owner / Business Owner DOIT initier l'examen préalable des risques relatifs à la vie privée dans REG04 avant le début de tout traitement de PII nouveau ou substantiellement modifié enregistré dans REG02.

4.1.2 [Both] Le Privacy Lead / PIMS Manager DOIT tenir à jour les critères d'examen préalable des risques relatifs à la vie privée dans REG04 avant la mise en service initiale du PIMS, puis annuellement.

4.1.3 [Controller] Le Process Owner / Business Owner DOIT réaliser l'examen préalable à la DPIA dans REG04 avant le début d'un traitement réalisé par un responsable du traitement qui satisfait aux critères d'examen préalable des risques relatifs à la vie privée.

4.1.4 [Processor] Le Vendor / Procurement Owner DOIT enregistrer les exigences d'assistance du client à la DPIA dans REG08 avant le début du traitement en tant que sous-traitant lorsque l'accord client ou l'instruction documentée exige un appui à la DPIA.

4.1.5 [Both] Le System Owner / Application Owner DOIT fournir dans REG04 les éléments de preuve relatifs à la conception du système, aux accès, à la sécurité, à la journalisation et aux flux de données avant l'approbation de l'appréciation des risques relatifs à la vie privée pour les systèmes nouveaux ou substantiellement modifiés traitant des PII.

4.1.6 [Both] Le Privacy Lead / PIMS Manager DOIT enregistrer le résultat de l'examen préalable et la justification de la décision relative à la DPIA complète dans REG04 avant que l'activité de traitement ne se poursuive.

4.2 Déclencheurs de DPIA et détermination de l'exigence

4.2.1 [Controller] Le Privacy Lead / PIMS Manager DOIT exiger une DPIA complète dans REG04 avant le début d'un traitement réalisé par un responsable du traitement susceptible d'engendrer un risque élevé.

4.2.2 [Controller] Le Process Owner / Business Owner DOIT soumettre au Privacy Lead / PIMS Manager, dans REG04, tout traitement impliquant une grande échelle, une surveillance systématique, du profilage, des décisions automatisées, des PII de catégories particulières, des données relatives aux condamnations pénales ou aux infractions, des personnes concernées vulnérables, une technologie innovante ou un traitement substantiellement modifié, avant le début du traitement.

4.2.3 [Controller] Le Data Protection Officer / Privacy Advisor DOIT consigner son avis dans REG04 avant l'approbation d'une décision imposant une DPIA complète pour un traitement à haut risque réalisé par un responsable du traitement.

4.2.4 [Both] Le Process Owner / Business Owner DOIT réexaminer les risques relatifs à la vie privée dans REG04 avant d'utiliser des PII pour une nouvelle finalité, d'ajouter un nouveau destinataire, d'introduire un nouveau sous-traitant ou sous-traitant ultérieur, de modifier l'architecture système ou de commencer un nouveau transfert international.

4.2.5 [Processor] Le Privacy Lead / PIMS Manager DOIT documenter dans REG08 si un appui à la DPIA par le sous-traitant est requis, dans un délai de 10 jours ouvrés à compter de la réception d'une demande d'assistance du client à la DPIA.

4.2.6 [Subprocessor] Le Vendor / Procurement Owner DOIT documenter dans REG08 les exigences d'assistance à la DPIA en amont avant le début du sous-traitement ultérieur lorsque l'accord avec le client amont ou le sous-traitant exige une telle assistance.

[... 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 aux risques pour la vie privée et aux DPIA

9.1.1 [All] Le Process Owner / Business Owner DOIT demander toute exception à la présente politique dans REG12 avant que l'écart ne se produise.

9.1.2 [All] Le Privacy Lead / PIMS Manager DOIT évaluer dans REG04 ou REG12 l'impact sur la vie privée, juridique, de certification, opérationnel et pour les personnes concernées de chaque exception demandée dans un délai de 10 jours ouvrés à compter de la demande.

9.1.3 [All] Le Data Protection Officer / Privacy Advisor DOIT consigner son avis dans REG12 avant l'approbation de toute exception affectant un traitement à haut risque, la réalisation d'une DPIA complète, une consultation préalable, un risque résiduel élevé relatif à la vie privée ou l'assistance du client à la DPIA.

9.1.4 [All] Top Management DOIT approuver dans REG12 les exceptions relatives aux risques pour la vie privée ou aux DPIA affectant un traitement à haut risque, le périmètre de certification, la consultation préalable ou un risque résiduel élevé non résolu relatif à la vie privée avant que l'exception ne prenne effet.

9.1.5 [All] Le Privacy Lead / PIMS Manager DOIT fixer dans REG12 une date d'expiration n'excédant pas 90 jours pour chaque exception approuvée relative aux risques pour la vie privée ou aux DPIA avant approbation.

9.1.6 [All] Le Process Owner / Business Owner DOIT clôturer ou réévaluer chaque exception relative aux risques pour la vie privée ou aux DPIA dans REG12 dans un délai de cinq jours ouvrés à compter de son expiration.

10. Application de la politique

10.1 Application relative aux risques pour la vie privée et aux DPIA

10.1.1 [All] Le Privacy Lead / PIMS Manager DOIT enregistrer dans REG12 comme non-conformité, dans un délai de cinq jours ouvrés à compter de son identification, tout élément de preuve REG04 relatif aux risques pour la vie privée ou aux DPIA qui est manquant, inexact, incomplet, en retard ou non approuvé.

10.1.2 [Controller] Le Process Owner / Business Owner DOIT suspendre tout nouveau traitement à haut risque réalisé par un responsable du traitement lorsque les éléments de preuve requis d'approbation de DPIA dans REG04 sont manquants avant le lancement.

10.1.3 [Both] Le System Owner / Application Owner DOIT bloquer la mise en production des systèmes traitant des PII lorsque les éléments de preuve requis de traitement des risques dans REG04 sont manquants avant l'approbation de la mise en production.

10.1.4 [Both] Le Vendor / Procurement Owner DOIT bloquer l'intégration d'un fournisseur, d'un sous-traitant, d'un sous-traitant ultérieur ou d'un dispositif de partage de données lorsque les éléments de preuve requis relatifs aux risques pour la vie privée ou à l'assistance à la DPIA dans REG04 sont manquants avant l'approbation de l'accord.

10.1.5 [All] Top Management DOIT examiner dans REG12, lors de la revue de direction, les non-conformités majeures non résolues relatives aux risques pour la vie privée ou aux DPIA.

10.1.6 [All] Le Privacy Lead / PIMS Manager DOIT escalader à Top Management dans REG12 les délais manqués répétés d'examen préalable dans REG04, de revue de DPIA ou de traitement des risques dans un délai de cinq jours ouvrés après la deuxième occurrence sur une période de 12 mois.

10.1.7 [All] Le Internal Audit / Compliance Reviewer DOIT vérifier dans REG12 l'efficacité des actions correctives relatives aux non-conformités portant sur les risques pour la vie privée et les DPIA lors du prochain audit planifié ou dans un délai de 60 jours suivant la clôture, selon la première éventualité.

11. Revue et maintenance

11.1 Revue et maintenance de la politique

11.1.1 [All] Le Privacy Lead / PIMS Manager DOIT revoir la présente politique dans REG12 annuellement et dans un délai de 30 jours suivant tout changement substantiel des exigences relatives aux risques pour la vie privée, aux DPIA, à la consultation préalable, à l'assistance du sous-traitant ou à la certification.

11.1.2 [All] Le Privacy Lead / PIMS Manager DOIT revoir annuellement dans REG12 les critères d'examen préalable dans REG04, les critères de déclenchement de DPIA, les critères de cotation des risques et les critères d'acceptation du risque résiduel.

11.1.3 [All] Le Data Protection Officer / Privacy Advisor DOIT 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 DOIT approuver dans REG12 les modifications substantielles de la présente politique avant publication.

11.1.5 [All] Le Privacy Lead / PIMS Manager DOIT mettre à jour REG03 et REG04 dans un délai de 15 jours ouvrés après les modifications approuvées de la politique qui modifient l'applicabilité des contrôles, les critères de risque ou les exigences d'examen préalable à la DPIA.

11.1.6 [All] Le Privacy Lead / PIMS Manager DOIT enregistrer dans REG11 la communication des modifications approuvées de la présente politique dans un délai de 30 jours suivant leur publication.

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 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 relative à la gestion du consentement et des préférences

12.7 PII06 - Politique relative à la gestion des droits des personnes concernées

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

12.9 PII09 - Politique relative à la collecte, à l'utilisation, à la divulgation et au partage de PII

12.10 PII10 - Politique relative à la conservation, à la suppression et à l'élimination de PII

12.11 PII11 - Politique relative à l'exactitude et à la qualité 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 relative à la sécurité des PII et au contrôle d'accès

12.15 PII15 - Politique de gestion des incidents et violations concernant les 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 La présente politique est cartographiée 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 appuient.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Cartographiée avec l'identification et la planification des actions relatives aux risques et opportunités pour la vie privée au moyen de critères d'examen préalable, de seuils de risque, de l'escalade et des données d'entrée de la revue de direction. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Cartographiée avec la réalisation de l'examen préalable des risques relatifs à la vie privée, l'appréciation des risques relatifs à la vie privée, la cotation des risques, la réappréciation et l'évaluation des déclencheurs de DPIA avant la poursuite de tout traitement nouveau ou substantiellement modifié. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Cartographiée avec la planification du traitement des risques relatifs à la vie privée, les mises à jour de l'applicabilité des contrôles, la mise en œuvre du traitement, l'acceptation du risque résiduel et l'articulation avec la SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Cartographiée avec les changements planifiés du PIMS et des traitements déclenchant une réappréciation des risques relatifs à la vie privée et une revue de DPIA. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Cartographiée avec les informations documentées maîtrisées pour l'examen préalable des risques relatifs à la vie privée, les éléments de preuve de DPIA, le traitement des risques, l'acceptation du risque résiduel, les décisions de consultation préalable, les

exceptions, les non-conformités et les éléments de preuve de revue de la politique. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Cartographiée avec l'exploitation des contrôles relatifs aux risques pour la vie privée et aux DPIA avant la mise en production, l'intégration, l'approbation du traitement, la clôture du traitement des risques et l'articulation avec les actions correctives. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Cartographiée avec l'appréciation opérationnelle des risques relatifs à la vie privée pour les traitements nouveaux ou modifiés ainsi que pour les changements liés aux systèmes, aux fournisseurs, aux transferts et aux incidents. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Cartographiée avec le traitement opérationnel des risques relatifs à la vie privée, l'attribution du traitement, la mise en œuvre du traitement, l'escalade des traitements en retard et la vérification de l'efficacité. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Cartographiée avec la surveillance et la mesure de la couverture de l'examen préalable, du statut des DPIA, des risques ouverts, des actions de traitement en retard, des actions fournisseurs, des actions de traitement de sécurité, des actions de réappréciation liées aux incidents et des constats d'audit. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Cartographiée avec la revue de direction des risques résiduels élevés relatifs à la vie privée, des actions de traitement en retard, du statut des DPIA complètes, des décisions de consultation préalable et des exceptions majeures relatives aux risques pour la vie privée. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Cartographiée avec les non-conformités relatives aux risques pour la vie privée et aux DPIA, les exceptions, l'ouverture d'actions correctives, l'escalade et la vérification de l'efficacité. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Cartographiée avec l'évaluation du besoin d'une analyse d'impact relative à la vie privée et, le cas échéant, sa mise en œuvre pour les traitements nouveaux ou modifiés réalisés par un responsable du traitement. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Cartographiée avec les registres des traitements soutenant les données d'entrée de l'appréciation des risques relatifs à la vie privée et des DPIA, notamment la finalité, les catégories, les systèmes, les destinataires, les transferts et les fournisseurs. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Cartographiée avec les accords clients du sous-traitant et les obligations d'assistance du client à la DPIA. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Cartographiée avec la fourniture par le sous-traitant des informations nécessaires à la conformité du client, y compris l'assistance à la DPIA et les éléments de preuve d'appui au client. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Cartographié avec les éléments de preuve de responsabilité relatifs à l'examen préalable à la DPIA, aux décisions de DPIA complète, au traitement des risques, à l'acceptation du risque résiduel, aux décisions de consultation préalable, aux exceptions, aux constats d'audit et aux actions correctives. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Cartographié avec la responsabilité du responsable du traitement concernant les mesures appropriées fondées sur les risques relatifs à la vie privée, la revue des risques résiduels élevés, l'approbation par la direction et la maintenance de la politique. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Cartographié avec les éléments de preuve de protection de la vie privée dès la conception et par défaut utilisés dans l'appréciation des risques et avant l'approbation de la mise en production. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Cartographié avec l'assistance des sous-traitants et sous-traitants ultérieurs à la DPIA, le traitement des instructions du client et les éléments de preuve de traitement des risques fournisseurs. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Cartographié avec les registres des traitements soutenant les données d'entrée de l'appréciation des risques relatifs à la vie privée et des DPIA. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Cartographié avec les données d'entrée relatives aux risques de sécurité des PII, la sélection des mesures de protection, le traitement des risques de sécurité et les mises à jour du statut des contrôles de sécurité. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Cartographié avec l'examen préalable à la DPIA, la détermination de l'exigence de DPIA complète, le contenu de la DPIA, l'avis du DPO, la revue et le blocage des traitements à haut risque sans approbation de DPIA requise. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Cartographié avec la prise de décision relative à la consultation préalable, l'avis du DPO, l'approbation par Top Management et les actions de poursuite, suspension, reconception ou consultation lorsqu'un risque résiduel élevé subsiste. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Cartographié avec les conseils et la surveillance du Data Protection Officer / Privacy Advisor lorsque applicable pour les décisions de DPIA, les traitements à haut risque, la consultation préalable et les modifications de la politique. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Cartographiée avec l'identification des contrôles relatifs à la vie privée, les mesures de protection de sécurité, la conformité en matière de vie privée, les éléments de preuve relatifs aux risques pour la vie privée, la surveillance et la revue. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Cartographiée avec le périmètre du processus de PIA, les bénéfices, la détermination des déclencheurs, la préparation, les données d'entrée de l'évaluation, les éléments de preuve des parties prenantes et la structure du rapport de DPIA conservés dans REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Cartographiée avec les exigences du programme de protection des PII, l'identification des exigences de protection des PII, la sélection des mesures de sécurité fondée sur les risques et l'articulation avec le traitement des risques relatifs à la vie privée. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Cartographiée avec les principes organisationnels de gestion des risques relatifs à la vie privée, le leadership, l'intégration, l'appréciation des risques, le traitement des risques, la surveillance et la revue, ainsi que l'enregistrement et le reporting. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].