					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII15-FS					Titre du document : **Politique de gestion des incidents et des violations de données à caractère personnel du secteur financier**							
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 7.4; Clause 7.5	Both	Supporting	Communications du PIMS et éléments de preuve documentés relatifs aux incidents
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Contrôle opérationnel, appréciation des risques relatifs à la vie privée et articulation avec le traitement des risques
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance, évaluation, non-conformité, action corrective et amélioration
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planification et préparation de la gestion des incidents pour le traitement des données à caractère personnel
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Réponse aux incidents de sécurité de l'information impliquant des données à caractère personnel
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Exigences légales, législatives, réglementaires et contractuelles, et protection des enregistrements
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Accord client du sous-traitant et soutien aux obligations du client

GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilité et obligations du responsable du traitement
GDPR	Article 26	Joint Controller	Supporting	Coordination des responsabilités relatives aux incidents entre responsables conjoints du traitement
GDPR	Article 28	Both	Supporting	Assistance du sous-traitant et obligations contractuelles du sous-traitant
GDPR	Article 32	Both	Supporting	Sécurité du traitement et capacité de détection des violations
GDPR	Article 33	Both	Primary	Notification des violations de données à caractère personnel et documentation des violations
GDPR	Article 34	Controller	Primary	Communication des violations de données à caractère personnel aux personnes concernées affectées
GDPR	Article 39	Conditional	Supporting	Conseil du DPO, surveillance, coopération et support du point de contact
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Processus de gestion des incidents liés aux TIC pour les entités financières relevant du champ d'application

DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Critères de classification des incidents liés aux TIC et des cybermenaces significatives
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Déclaration des incidents majeurs liés aux TIC et notification des cybermenaces significatives
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Contenu des déclarations, délais, modèles et procédures
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Déclaration des incidents significatifs le cas échéant
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Principes de sécurité de l'information et de conformité en matière de vie privée
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilités de réponse aux incidents relatifs aux données à caractère personnel et signalement des événements
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planification, évaluation, réponse, retours d'expérience et collecte des éléments de preuve relatifs aux incidents
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Cycle de vie du processus de gestion des incidents
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Politique, plan, sensibilisation, tests et retours

				d'expérience relatifs aux incidents
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Opérations de détection, notification, triage, analyse, réponse et rapport
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Attentes relatives à la notification par le sous-traitant cloud public et à l'enregistrement des violations

1. Champ d’application

1.1 La présente politique définit les exigences applicables à l'identification, au signalement, au triage, à la classification, à l'évaluation, au confinement, à la notification, à la documentation, à la clôture et à l'amélioration à la suite d'incidents relatifs aux données à caractère personnel et de violations de données à caractère personnel dans les domaines d’application du PIMS du secteur financier.

1.2 **Avis de mise en œuvre :** La présente politique constitue une variante de remplacement de PII15 pour le secteur financier. Elle ne doit pas être mise en œuvre simultanément avec PII15 pour le même domaine d’application du PIMS, la même unité opérationnelle, le même produit, le même environnement client, le même service réglementé ou le même périmètre d’éléments de preuve. Les organisations doivent sélectionner soit PII15, soit PII15-FS pour le même périmètre afin d'éviter les obligations de gestion des incidents en double, les registres en double et les travaux d’éléments de preuve d’audit en double.

1.3 La présente politique s'applique :

1.3.1 à l'organisation agissant en qualité de responsable du traitement dans un contexte de secteur financier ;

1.3.2 à l'organisation agissant en qualité de responsable conjoint du traitement lorsqu'une coordination des responsabilités relatives à un incident ou à une violation est requise ;

1.3.3 à l'organisation agissant en qualité de sous-traitant pour des clients du secteur financier ;

1.3.4 à l'organisation agissant en qualité de sous-traitant ultérieur pour des clients du secteur financier ou des sous-traitants en amont ;

1.3.5 aux systèmes, applications, services, processus, fournisseurs, sous-traitants, sous-traitants ultérieurs et tiers qui traitent, stockent, transmettent, prennent en charge, consultent ou affectent autrement des données à caractère personnel dans le domaine d’application du PIMS du secteur financier.

1.4 La présente politique utilise REG10 - Registre des incidents et violations de données à caractère personnel comme objet principal d’éléments de preuve pour la gestion des incidents et violations de données à caractère personnel du secteur financier.

1.5 La présente politique utilise les objets d’éléments de preuve de support comme suit :

1.5.1 REG01 pour le domaine d’application du PIMS, les parties intéressées applicables et le contexte sectoriel, client, contractuel et déclaratif.

1.5.2 REG02 pour les activités de traitement, catégories de données à caractère personnel, catégories de personnes concernées, finalités, systèmes et services affectés.

1.5.3 REG03 pour la Déclaration d’applicabilité et les mises à jour relatives à l'applicabilité des contrôles, y compris le remplacement de PII15 par PII15-FS pour le même périmètre.

1.5.4 REG04 pour les liens avec les risques relatifs à la vie privée, la DPIA, le risque résiduel et le traitement des risques.

1.5.5 REG08 pour les éléments de preuve relatifs aux interfaces d'incident avec les sous-traitants, sous-traitants ultérieurs, clients, fournisseurs et tiers.

1.5.6 REG09 pour l'articulation avec les transferts internationaux lorsqu'un incident affecte un traitement transfrontalier.

1.5.7 REG11 pour les éléments de preuve relatifs à la formation, à la sensibilisation et à la compétence en réponse aux incidents.

1.5.8 REG12 pour les éléments de preuve relatifs à l'audit, aux non-conformités, aux actions correctives, à la revue de direction et à l'amélioration.

1.6 La présente politique s'appuie sur les politiques PIMS associées pour les contrôles spécialisés :

1.6.1 PII03 régit l'inventaire des traitements et les enregistrements relatifs à la base légale.

1.6.2 PII04 régit la mention d'information et les contrôles de transparence en dehors des communications propres aux violations.

1.6.3 PII06 régit les demandes d'exercice des droits des personnes concernées qui surviennent avant, pendant ou après un incident.

1.6.4 PII07 régit la méthodologie d'appréciation des risques relatifs à la vie privée et de DPIA.

1.6.5 PII08 régit les contrôles de protection de la vie privée dès la conception et par défaut.

1.6.6 PII10 régit les contrôles de conservation, de suppression et d'élimination.

1.6.7 PII12 régit les contrôles des relations avec les sous-traitants, sous-traitants ultérieurs, fournisseurs et tiers en matière de protection des données.

1.6.8 PII13 régit les outils de transfert international de données à caractère personnel et les enregistrements des risques liés aux transferts.

1.6.9 PII14 régit les contrôles préventifs et détectifs de sécurité des données à caractère personnel et de contrôle d'accès.

1.6.10 PII16 régit la formation, la sensibilisation et la compétence en matière de vie privée.

1.6.11 PII17 régit les informations documentées et la gestion des éléments de preuve.

1.6.12 PII18 régit la surveillance, l'audit interne, la revue de direction, les non-conformités, les actions correctives et l'amélioration continue.

1.6.13 PII23 régit les contrôles du sous-traitant cloud de données à caractère personnel lorsque les obligations de sous-traitant cloud relèvent du périmètre.

1.7 Aux fins de la présente politique :

1.7.1 « incident relatif aux données à caractère personnel » désigne un événement suspecté ou confirmé qui a affecté, peut avoir affecté ou pourrait raisonnablement affecter la confidentialité, l'intégrité, la disponibilité, le traitement licite ou le traitement autorisé de données à caractère personnel.

1.7.2 « violation de données à caractère personnel » désigne un incident confirmé relatif aux données à caractère personnel impliquant la destruction, la perte, l'altération, la divulgation, l'accès, l'indisponibilité ou la compromission, de manière non autorisée, illicite, accidentelle ou non intentionnelle, de données à caractère personnel.

1.7.3 « incident du secteur financier relatif aux données à caractère personnel » désigne un incident relatif aux données à caractère personnel qui affecte, peut affecter ou est raisonnablement lié à des services financiers réglementés, des clients du secteur financier, des contreparties financières, des transactions financières, des opérations financières ou un traitement de données à caractère personnel du secteur financier.

1.7.4 « incident majeur du secteur financier » désigne un incident du secteur financier relatif aux données à caractère personnel ou un incident lié aux TIC connexe qui satisfait aux critères documentés de matérialité ou de déclaration dans REG10.

1.7.5 « cybermenace significative » désigne une cybermenace enregistrée dans REG10 susceptible d'affecter de manière substantielle les services du secteur financier, le traitement de données à caractère personnel, les clients, les contreparties ou les opérations relevant du périmètre.

1.7.6 « évaluation d'une violation de données à caractère personnel » désigne l'évaluation documentée visant à déterminer si un incident relatif aux données à caractère personnel constitue une violation de données à caractère personnel, quelles données à caractère personnel et quelles personnes concernées sont affectées, quels risques peuvent survenir,

quelles notifications ou communications sont requises et quelles actions correctives sont nécessaires.

1.7.7 « prise de connaissance » désigne le moment auquel l'organisation dispose d'un degré raisonnable de certitude qu'un incident de sécurité ou de vie privée s'est produit et que des données à caractère personnel ont été ou peuvent avoir été compromises.

1.7.8 « incident à fort impact du secteur financier relatif aux données à caractère personnel » désigne un incident relatif aux données à caractère personnel impliquant un traitement à haut risque, des catégories particulières de données ou des données à caractère personnel hautement sensibles, des données à caractère personnel à grande échelle, des personnes vulnérables, des clients réglementés, une interruption substantielle de service, des contreparties financières, des transactions financières, un impact multi-juridictionnel, une compromission d'accès à privilèges, une exposition publique, un rançongiciel, une indisponibilité de service ou un impact opérationnel, client, financier ou réputationnel significatif.

1.7.9 « modification substantielle relative à un incident » désigne toute information nouvelle ou modifiée affectant le périmètre de l'incident, sa gravité, les catégories de données à caractère personnel, l'impact sur les personnes concernées, l'impact sur les services, la classification sectorielle financière, la décision de notification, l'impact client, la cause racine, le confinement, le rétablissement, l'action corrective ou les obligations de déclaration externe.

2. Objet

2.1 La présente politique a pour objet de garantir que les incidents et violations de données à caractère personnel dans les contextes du secteur financier sont traités de manière cohérente, rapide, licite, sécurisée et compatible avec les exigences d'audit.

2.2 La présente politique soutient la responsabilité en exigeant que les incidents et violations de données à caractère personnel du secteur financier soient enregistrés dans REG10 et reliés aux enregistrements des traitements affectés, aux risques relatifs à la vie privée, aux relations avec les sous-traitants et sous-traitants ultérieurs, aux enregistrements de transfert, aux actions correctives, aux enregistrements de formation, aux décisions de déclaration sectorielle financière et aux éléments de preuve de revue de direction lorsque cela est déclenché.

2.3 La présente politique garantit que les obligations du responsable du traitement, du responsable conjoint du traitement, du sous-traitant et du sous-traitant ultérieur sont traitées au moyen de règles d'applicabilité distinctes, tout en maintenant un modèle intégré unique d’éléments de preuve relatifs aux incidents et violations du secteur financier.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 garantir que les incidents suspectés du secteur financier relatifs aux données à caractère personnel sont signalés et enregistrés rapidement ;

3.1.2 garantir que les incidents du secteur financier relatifs aux données à caractère personnel sont triés et classifiés au moyen de critères cohérents en matière de vie privée, de sécurité, d'exploitation et de secteur ;

3.1.3 garantir que les évaluations de violation tiennent compte des données à caractère personnel, des personnes concernées, des systèmes, des services, des activités de traitement, des sous-traitants, des sous-traitants ultérieurs, des transferts, des risques, des clients, des contreparties et des actions correctives affectés ;

3.1.4 garantir que les décisions de notification du responsable du traitement et de communication aux personnes concernées sont documentées ;

3.1.5 garantir que les notifications de violation par le sous-traitant et le sous-traitant ultérieur aux clients ou aux parties en amont sont effectuées sans retard indu et conformément aux accords applicables ;

3.1.6 garantir que les déclencheurs de déclaration sectorielle financière sont évalués, documentés et suivis le cas échéant ;

3.1.7 garantir que les éléments de preuve sont préservés et protégés pendant le traitement de l'incident ;

3.1.8 garantir que le confinement, l'éradication, le rétablissement et la validation sont suivis dans REG10 ;

3.1.9 garantir que les cybermenaces significatives et les incidents majeurs du secteur financier sont orientés vers les workflows de décision et de déclaration appropriés ;

3.1.10 garantir que les retours d'expérience sur les incidents donnent lieu à des actions correctives, à de la formation, à l'amélioration des contrôles et à une revue de direction ;

3.1.11 garantir que les enregistrements d'incident et de violation sont disponibles pour l'audit, la revue de direction, l'assurance client et la revue réglementaire le cas échéant ;

3.1.12 garantir que PII15-FS remplace PII15 pour le même périmètre sectoriel financier et ne duplique pas les travaux d'éléments de preuve de PII15.

4. Énoncés de politique

4.1 Activation de la variante, préparation et réception

4.1.1 [Conditional] The Privacy Lead / PIMS Manager DOIT documenter l'activation de PII15-FS dans REG01 et REG03 avant que la présente politique ne soit utilisée pour un domaine d'application du PIMS du secteur financier.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager DOIT documenter dans REG03 et REG12 que PII15 n'est pas mise en œuvre simultanément pour le même domaine d'application du PIMS du secteur financier avant l'approbation de PII15-FS.

4.1.3 [All] The Incident Response Coordinator DOIT enregistrer chaque incident suspecté du secteur financier relatif aux données à caractère personnel signalé ou détecté dans REG10 dans un délai d'un jour ouvré à compter de sa réception, ou plus tôt lorsqu'un délai applicable de notification, client ou de déclaration peut être déclenché.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager DOIT maintenir les critères de traitement des incidents et violations de données à caractère personnel du secteur financier dans REG10 au moins une fois par an et après toute modification substantielle du domaine d'application du PIMS, du contexte juridique, des obligations client, des obligations contractuelles, du contexte de déclaration sectorielle ou d'un traitement à haut risque.

4.1.5 [Both] The Information Security Lead DOIT confirmer les exigences de préservation des éléments de preuve relatifs à l'incident dans REG10 dans les 24 heures suivant le moment où un incident suspecté affecte un système, un service ou une application traitant des données à caractère personnel.

4.1.6 [Conditional] The Vendor / Procurement Owner DOIT maintenir les exigences de contact et d'acheminement des éléments de preuve relatives aux incidents des tiers du secteur financier dans REG08 avant l'intégration et au moins une fois par an pour les sous-traitants, sous-traitants ultérieurs, fournisseurs et prestataires de déclaration externalisés relevant du périmètre.

4.2 Classification et évaluation d'une violation de données à caractère personnel

4.2.1 [All] The Incident Response Coordinator DOIT classifier chaque entrée REG10 dans les 24 heures suivant la réception comme événement non lié aux données à caractère personnel,

incident suspecté relatif aux données à caractère personnel, incident confirmé relatif aux données à caractère personnel, violation confirmée de données à caractère personnel, incident du secteur financier relatif aux données à caractère personnel, incident majeur du secteur financier, cybermenace significative ou entrée en attente de classification.

4.2.2 [Conditional] The Information Security Lead DOIT évaluer dans REG10 les services, clients, contreparties, transactions, indisponibilité des services, extension géographique, perte de données, criticité du service et impact économique affectés lorsqu'un incident relatif aux données à caractère personnel peut affecter les services ou opérations du secteur financier.

4.2.3 [Both] The Privacy Lead / PIMS Manager DOIT identifier l'activité de traitement, les catégories de données à caractère personnel, les catégories de personnes concernées, les systèmes, les sous-traitants, les sous-traitants ultérieurs, les lieux de transfert et les risques relatifs à la vie privée affectés dans REG02, REG04, REG08, REG09 et REG10 avant que la décision relative à la notification d'une violation de données à caractère personnel ne soit finalisée.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor DOIT évaluer le risque pour les personnes concernées affectées pour chaque violation de données à caractère personnel confirmée ou raisonnablement suspectée, et enregistrer la recommandation de notification, la justification du risque et le conseil dans REG10 avant que la décision de notification externe ne soit prise.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager DOIT enregistrer la répartition des responsabilités relatives à l'incident entre responsables conjoints du traitement dans REG08 et REG10 dans les 24 heures suivant l'identification d'une responsabilité partagée pour une violation de données à caractère personnel suspectée ou confirmée.

4.2.6 [Processor] The Privacy Lead / PIMS Manager DOIT évaluer les instructions du client, les obligations contractuelles de notification et les obligations de coopération dans REG08 et REG10 dans les 24 heures suivant le moment où une violation de données à caractère personnel suspectée ou confirmée affecte un traitement réalisé en qualité de sous-traitant.

4.2.7 [Subprocessor] The Vendor / Procurement Owner DOIT identifier la chaîne de notification en amont et l'acheminement requis des éléments de preuve dans REG08 et REG10 dans les 24 heures suivant le moment où un incident suspecté ou confirmé relatif aux données à caractère personnel affecte un traitement réalisé en qualité de sous-traitant ultérieur.

[... 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] The Privacy Lead / PIMS Manager DOIT enregistrer toute exception à la présente politique dans REG12 avant sa mise en œuvre, ou dans les 24 heures suivant une action d'urgence lorsque l'approbation préalable n'était pas possible.

9.1.2 [Conditional] Top Management DOIT approuver toute exception qui affecte de manière substantielle le calendrier de notification des violations, le calendrier de déclaration du secteur financier, la communication publique, l'engagement client, la préservation des éléments de preuve ou le risque pour les personnes concernées avant la clôture de l'incident, les éléments de preuve d'approbation étant conservés dans REG10 et REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor DOIT documenter les conseils pour toute notification retardée, décision de non-notification, exception de déclaration ou approche exceptionnelle de communication avant la clôture de l'incident, les conseils étant conservés dans REG10.

9.1.4 [Both] The Vendor / Procurement Owner DOIT enregistrer dans REG08 et REG12 les exceptions relatives aux fournisseurs, sous-traitants, sous-traitants ultérieurs, clients ou prestataires externalisés affectant la réponse aux incidents du secteur financier dans les cinq jours ouvrés suivant l'identification de l'exception.

9.1.5 [All] The Privacy Lead / PIMS Manager DOIT revoir au moins mensuellement les exceptions ouvertes à la présente politique jusqu'à leur clôture, le statut de revue étant conservé dans REG12.

10. Application de la politique

10.1.1 [All] The Process Owner / Business Owner DOIT escalader au Privacy Lead / PIMS Manager tout défaut de signalement d'un incident suspecté du secteur financier relatif aux données à caractère personnel, de préservation des éléments de preuve, de suivi des actions assignées ou de coopération à l'évaluation de la violation dans un délai de deux jours ouvrés après découverte, les éléments de preuve étant conservés dans REG12.

10.1.2 [Both] The Incident Response Coordinator DOIT escalader au Privacy Lead / PIMS Manager tout signalement tardif, classification manquée, élément de preuve manquant, escalade manquée ou action de confinement en retard dans un délai d'un jour ouvré après identification du problème, les éléments de preuve étant conservés dans REG10 et REG12.

10.1.3 [Both] The Privacy Lead / PIMS Manager DOIT enregistrer une non-conformité REG12 lorsqu'un manquement à la présente politique affecte la réception, le triage, le confinement, la notification, la déclaration, l'intégrité des éléments de preuve, la communication ou l'action corrective relatifs aux incidents.

10.1.4 [Both] The Vendor / Procurement Owner DOIT engager une remédiation du fournisseur, du sous-traitant, du sous-traitant ultérieur ou du prestataire externalisé via REG08 et REG12 dans les cinq jours ouvrés lorsqu'un tiers ne respecte pas les obligations convenues en matière d'incident, de violation, d’éléments de preuve ou de déclaration.

10.1.5 [Conditional] Top Management DOIT examiner les non-conformités substantielles ou récurrentes à PII15-FS lors de la prochaine revue de direction programmée, les décisions et actions requises étant conservées dans REG12.

10.1.6 [All] The Privacy Lead / PIMS Manager DOIT déclencher une formation de remédiation dans REG11 dans les 30 jours calendaires lorsqu'une non-conformité à la politique implique la sensibilisation au rôle, un signalement tardif, un défaut d'escalade, un défaut de traitement des éléments de preuve ou un défaut de communication.

11. Revue et maintenance

11.1.1 [Conditional] The Privacy Lead / PIMS Manager DOIT revoir la présente politique au moins une fois par an et enregistrer le résultat de la revue, les modifications requises et le statut d'approbation dans REG12.

11.1.2 [Conditional] The Incident Response Coordinator DOIT déclencher une revue post-incident de la présente politique dans les 30 jours calendaires suivant la clôture de tout incident à fort impact du secteur financier relatif aux données à caractère personnel, violation confirmée de données à caractère personnel, incident majeur du secteur financier ou cybermenace significative, les éléments de preuve de revue étant conservés dans REG10 et REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager DOIT revoir la présente politique dans les 30 jours calendaires suivant la prise de connaissance d'une modification substantielle des exigences de déclaration d'incident légales, sectorielles, client, contractuelles, relatives aux sous-traitants, aux sous-traitants ultérieurs, aux modèles de déclaration, aux délais de déclaration ou aux transferts, les éléments de preuve de revue étant conservés dans REG01, REG08, REG09 et REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer DOIT revoir la mise en œuvre de la présente politique au moins une fois par an dans le cadre du programme d'audit interne du PIMS, les constats d'audit et actions correctives étant conservés dans REG12.

11.1.5 [Conditional] Top Management DOIT examiner les tendances des incidents, les violations significatives, la performance de déclaration, les actions correctives en retard et l'efficacité de la politique lors de la revue de direction programmée, les livrables étant conservés dans REG12.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager DOIT revoir la relation de remplacement entre PII15-FS et PII15 au moins une fois par an et après toute modification du périmètre du PIMS afin de vérifier que les deux politiques ne sont pas mises en œuvre pour le même périmètre du secteur financier, les éléments de preuve de revue étant conservés dans REG03 et REG12.

12. Politiques associées

12.1 La présente politique doit être lue avec :

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

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

12.4 PII03 - Politique relative à l'inventaire des traitements de données à caractère personnel et aux bases légales

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

12.6 PII06 - Politique de gestion des droits des personnes concernées

12.7 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA

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

12.9 PII10 - Politique de conservation, de suppression et d'élimination des données à caractère personnel

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

12.11 PII13 - Politique de transfert international de données à caractère personnel

12.12 PII14 - Politique de sécurité des données à caractère personnel et de contrôle d'accès

12.13 PII16 - Politique de formation, sensibilisation et compétence en matière de vie privée

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

12.16 PII23 - Politique relative aux sous-traitants cloud de données à caractère personnel, lorsque les obligations du sous-traitant cloud du secteur financier relèvent du périmètre

12.17 PII15 - La Politique de gestion des incidents et violations de données à caractère personnel est la politique de référence relative aux incidents et violations. PII15-FS est une variante de remplacement de PII15 pour le secteur financier. PII15 et PII15-FS ne doivent pas être mises en œuvre simultanément pour le même domaine d'application du PIMS, la même unité opérationnelle, le même produit, le même environnement client, le même service réglementé ou le même périmètre d'éléments de preuve.

13. Normes et référentiels de référence

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].