					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P37					Titre du document : **Politique de conformité juridique et réglementaire**							
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**

1. Objet

1.1 La présente politique établit le cadre obligatoire d'identification, de gestion et de respect de l'ensemble des obligations juridiques, réglementaires et contractuelles applicables à la sécurité de l'information, à la protection des données et aux activités opérationnelles de l'organisation.

1.2 Elle vise à prévenir toute non-conformité susceptible d'entraîner des amendes, une mise en cause de la responsabilité juridique, une perturbation des activités, une atteinte à la réputation ou des mesures d'exécution prises par les autorités de régulation.

1.3 La présente politique soutient l'intégration des obligations de conformité dans la gouvernance, les processus de gestion des risques, les processus opérationnels, les cycles de vie des projets et la conception des systèmes.

1.4 Elle exige que toutes les obligations applicables — dans l'ensemble des juridictions, secteurs d'activité et périmètres réglementaires concernés — soient clairement documentées, évaluées, surveillées et appliquées au sein de l'organisation.

2. Champ d'application

2.1 La présente politique s'applique à tous les départements, fonctions, unités opérationnelles et à toute personne agissant pour le compte de l'organisation, y compris :

2.1.1 les employés permanents et temporaires ;

2.1.2 les prestataires, consultants et stagiaires ;

2.1.3 les fournisseurs tiers, les sous-traitants de données ou les partenaires traitant les données, les systèmes ou les obligations réglementaires de l'organisation ;

2.1.4 tout processus métier, projet ou initiative soumis à une exigence juridique ou réglementaire.

2.2 Les domaines de conformité régis par la présente politique comprennent notamment :

2.2.1 les obligations en matière de sécurité de l'information et de cybersécurité (p. ex. ISO/IEC 27001, NIS2, DORA) ;

2.2.2 la législation relative à la protection des données et au respect de la vie privée (p. ex. RGPD, lois sectorielles en matière de vie privée) ;

2.2.3 les réglementations sectorielles (p. ex. finance, médical, automobile, défense) ;

2.2.4 les obligations contractuelles résultant d'accords de non-divulgation, d'accords de niveau de service (SLA) ou d'accords de traitement conclus avec des tiers ;

2.2.5 les exigences juridiques relatives au signalement des incidents, aux interactions avec les autorités répressives et aux transferts internationaux de données.

3. Objectifs

3.1 Garantir que l'ensemble des lois, réglementations, normes et obligations contractuelles applicables soient identifiées, documentées, interprétées et appliquées dans toute l'organisation.

3.2 Intégrer les exigences juridiques et réglementaires dans le SMSI de l'organisation, les processus de gestion des risques, les accords fournisseurs et la conception des produits et services.

3.3 Prévoir un mécanisme de surveillance proactive des évolutions réglementaires et de mise à jour corrélative des contrôles et de la documentation.

3.4 Définir une responsabilité claire pour la supervision de la conformité, l'escalade des manquements, la gestion des exceptions et les déclarations externes.

3.5 Garantir l'auditabilité et la robustesse de la position juridique et réglementaire de l'organisation lors des inspections, enquêtes ou revues de certification.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Porte la responsabilité stratégique de l'alignement juridique et réglementaire à l'échelle de l'organisation.

4.1.2 Examine et approuve les décisions de conformité à haut risque, y compris les acceptations de risque et les contentieux.

4.2 Responsable de la conformité / service juridique / conseiller juridique

4.2.1 Tient à jour le registre des obligations de conformité, recensant l'ensemble des lois, normes, certifications et clauses contractuelles applicables.

4.2.2 Réalise des évaluations d'impact juridique pour les nouveaux services, marchés ou flux de données.

4.2.3 Fournit l'interprétation de référence des lois et des normes.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Exigences de revue et de mise à jour

9.1 Revue annuelle de la politique

9.1.1 La présente politique doit faire l'objet d'une revue au moins une fois par année civile afin de :

9.1.1.1 garantir le maintien de l'alignement avec les lois, normes sectorielles et cadres réglementaires mis à jour ;

9.1.1.2 valider l'efficacité opérationnelle au regard des constats d'audit et de l'historique des incidents ;

9.1.1.3 refléter les changements organisationnels (p. ex. nouvelles juridictions, nouveaux systèmes ou nouvelles lignes d'activité).

9.2 Revues déclenchées par un événement

9.2.1 Des revues intermédiaires doivent être engagées lorsque :

9.2.2 une nouvelle exigence juridique ou réglementaire est adoptée ou mise à jour ;

9.2.3 un incident de conformité ou un audit met en évidence des insuffisances dans la politique ;

9.2.4 l'organisation entre sur un nouveau marché ou lance une nouvelle activité de service régie par des cadres de conformité distincts ;

9.2.5 les tendances en matière d'application ou les orientations des autorités de régulation indiquent une évolution du niveau de risque.

9.3 Responsabilité et approbation

9.3.1 Le service juridique et le responsable de la conformité assument conjointement la responsabilité de coordonner le processus de revue.

9.3.2 Les modifications finales de la politique doivent être approuvées par la haute direction et consignées dans le registre des modifications de politique, avec les références associées au contrôle des changements et les plans de communication.

9.4 Gestion des versions et communication

9.4.1 Toute version mise à jour de la présente politique doit :

9.4.1.1 inclure un résumé des principales modifications ;

9.4.1.2 être redistribuée par les canaux officiels (p. ex. portail des politiques, LMS, lettres d'information internes) ;

9.4.1.3 exiger une prise de connaissance des membres du personnel concernés, en particulier ceux exerçant des fonctions juridiques, opérationnelles, de sécurité et de gestion des fournisseurs.

10. Politiques associées et articulations

10.1 La présente politique s'applique en articulation avec les politiques suivantes du SMSI de l'organisation et les renforce :

10.1.1 P1 – Politique de sécurité de l'information : établit les principes de gouvernance de référence garantissant que l'ensemble des politiques de sécurité de l'information — y compris la conformité — sont alignées sur les exigences stratégiques de l'activité et les exigences réglementaires.

10.1.2 P2 – Politique relative aux rôles et responsabilités de gouvernance : définit les pouvoirs décisionnels, y compris les rôles juridiques et de conformité chargés de la supervision réglementaire et de la responsabilisation.

10.1.3 P6 – Politique de gestion des risques : soutient l'évaluation, l'attribution et l'atténuation des risques de conformité juridique et réglementaire à l'échelle de l'organisation.

10.1.4 P8 – Politique de sensibilisation et de formation à la sécurité de l'information : veille à ce que l'ensemble du personnel soit informé de ses responsabilités en matière de conformité et reçoive une formation adaptée à son rôle.

10.1.5 P12 – Politique de gestion des actifs : renforce les obligations juridiques relatives à la gestion et à la protection des actifs réglementés ou contractuels, y compris ceux comportant des données à caractère personnel et relevant d'infrastructures critiques.

10.1.6 P30 – Politique de réponse aux incidents : encadre les notifications juridiques obligatoires (p. ex. article 33 du RGPD) et les procédures d'escalade en cas de manquement à la conformité ou d'événement réglementaire.

10.1.7 P33 – Politique d'audit et de surveillance de la conformité : prévoit des activités d'assurance structurées — y compris les tests de contrôle et la collecte des éléments probants — requises pour la vérification interne et externe de la conformité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Clause 4.2 – Compréhension des besoins et attentes des parties intéressées : exige l'identification et l'intégration des exigences juridiques et réglementaires dans le SMSI.

11.1.2 Clause 5.1 – Leadership et engagement : impose à la direction la responsabilité d'établir et de maintenir la conformité juridique dans toute l'organisation.

11.1.3 Clause 5.3 – Rôles, responsabilités et autorités au sein de l'organisation : garantit la clarté des rôles relatifs à la supervision juridique et à la conformité réglementaire.

11.1.4 Annexe A, contrôle 5.36 – Conformité aux exigences juridiques, statutaires, réglementaires et contractuelles : établit l'obligation d'identifier et de respecter les obligations résultant des lois, réglementations et contrats.

11.2 ISO/IEC 27002

11.2.1 Contrôle 5.36 : détaille les modalités de mise en œuvre relatives au maintien d'un registre des obligations de conformité, à la validation des exigences réglementaires et à la conservation structurée des éléments probants.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politique et procédures de planification de la sécurité : exige que les obligations de conformité soient intégrées dans les structures de gouvernance et la documentation.

11.3.2 PM-1 – Plan du programme de sécurité de l'information : impose les contrôles réglementaires comme composante du programme global de sécurité.

11.3.3 CA-7 – Surveillance continue : soutient la supervision de l'efficacité des contrôles au regard des exigences juridiques et des politiques.

11.3.4 AU-9 – Protection des informations d'audit : garantit que les journaux et enregistrements d'audit de conformité sont protégés et disponibles pour inspection.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 5 – Principes relatifs au traitement : exige un traitement licite des informations, la transparence et la responsabilité.

11.4.2 Article 6 – Licéité du traitement : impose des bases légales appropriées pour toutes les activités de traitement des données.

11.4.3 Article 24 – Responsabilité du responsable du traitement : établit une responsabilité directe pour garantir la conformité réglementaire.

11.4.4 Article 32 – Sécurité du traitement : exige la mise en œuvre de mesures techniques et organisationnelles appropriées.

11.4.5 Article 33 – Notification d'une violation : exige que les violations de données à caractère personnel soient notifiées dans un délai de 72 heures aux autorités compétentes.

11.5 Directive NIS2 de l'UE (2022/2555)

11.5.1 Articles 20–21 : imposent aux entités essentielles et importantes de mettre en œuvre une gouvernance documentée, des dispositifs de conformité juridique et une revue continue des risques juridiques.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 5(2) – Cadre de gestion des risques liés aux TIC : exige l'intégration de la conformité juridique dans les fonctions étendues de gestion des risques et de supervision.

11.6.2 Article 19 – Risque lié aux tiers en matière de TIC : impose des exigences juridiques spécifiques pour la gestion des obligations contractuelles et réglementaires impliquant des fournisseurs externes et des plateformes.

11.7 COBIT 2019

11.7.1 APO12 – Gérer les risques : intègre la conformité juridique et réglementaire comme composante critique de la gouvernance des risques de l'organisation.

11.7.2 MEA03 – Surveiller, évaluer et apprécier la conformité aux exigences externes : définit une surveillance continue, la gestion des exceptions et la préparation à l'audit pour toutes les formes d'obligations réglementaires.