					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P37S					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**

Alignement sur les normes et réglementations

Norme/Réglementation	Clause/Article	Commentaire
ISO/IEC 27001:2022	Articles 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Mesure 5	
NIST SP 800-53 Rév. 5	PL-1, PL-2, PM-1, CA-1, AU-1	
RGPD de l'UE	Articles 5, 6, 32, 33	
NIS2 de l'UE	Articles 21(2)(a), 21(2)(f), 23	
DORA de l'UE	Articles 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Objet

1.1 La présente politique définit l'approche de l'organisation pour identifier, respecter et démontrer le respect des obligations juridiques, réglementaires et contractuelles.

1.2 Elle établit des responsabilités claires et des mesures concrètes afin d'aider l'entreprise à satisfaire à ses obligations de conformité, y compris en matière de protection des données, de référentiels de cybersécurité, d'accords clients et de normes de certification.

1.3 Elle garantit que, même en l'absence d'une équipe conformité dédiée, l'entreprise peut maintenir des opérations conformes aux exigences légales, réagir de manière appropriée aux incidents et conserver un niveau complet de préparation à l'audit.

1.4 La présente politique est essentielle pour permettre la certification ISO/IEC 27001:2022 et répondre aux attentes externes des clients, des autorités de régulation et des partenaires.

2. Champ d’application

2.1 La présente politique s'applique à :

2.1.1 l'ensemble des employés, prestataires indépendants, sous-traitants et fournisseurs tiers ;

2.1.2 l'ensemble des services, opérations, systèmes et activités de traitement des données pour lesquels l'organisation doit respecter des exigences juridiques ou contractuelles ;

2.1.3 l'ensemble des sites et équipements utilisés pour traiter les informations de l'entreprise, qu'ils soient exploités dans les locaux, à distance ou dans des environnements cloud.

2.2 La présente politique couvre :

2.2.1 les lois relatives à la protection des données, telles que le RGPD de l'UE ;

2.2.2 les réglementations de cybersécurité telles que la directive NIS2 de l'UE ;

2.2.3 les obligations sectorielles spécifiques, le cas échéant ;

2.2.4 les contrats clients, les accords de non-divulgation et les clauses d'audit ;

2.2.5 les certifications volontaires (par ex. ISO 27001) et les politiques internes dont l'application est requise pour assurer la conformité.

3. Objectifs

3.1 Établir les responsabilités : attribuer clairement la responsabilité de la surveillance, de la mise à jour et de l'application des obligations juridiques, réglementaires et contractuelles.

3.2 Protéger l'entreprise : réduire au minimum le risque de non-conformité, de sanctions financières, de violations de données et d'atteinte à la réputation.

3.3 Assurer la préparation à l'audit : maintenir des enregistrements vérifiables démontrant comment l'organisation satisfait à ses obligations de conformité.

3.4 Soutenir l'intégration des politiques : veiller à ce que les obligations juridiques et réglementaires soient appliquées de manière cohérente dans l'ensemble des politiques et des processus.

3.5 Gérer les exceptions en toute transparence : veiller à ce que toute exception de conformité soit documentée, justifiée et approuvée afin de limiter l'exposition juridique.

4. Rôles et responsabilités

4.1 Directeur général (DG)

4.1.1 Assume la responsabilité globale de la conformité juridique et réglementaire de l'organisation.

4.1.2 Tient le registre de conformité et veille à sa mise à jour.

4.1.3 Examine les contrats clients et veille au suivi et à l'application des obligations spécifiques.

4.1.4 N'approuve les exceptions aux obligations de conformité que lorsqu'elles sont juridiquement justifiables et assorties de mesures compensatoires.

4.2 Conseillers externes (par ex. juridiques, informatiques ou consultants en conformité)

4.2.1 Assistent le DG dans l'identification des lois, certifications et obligations applicables (par ex. RGPD, NIS2, ISO 27001).

4.2.2 Fournissent des orientations sur l'interprétation des nouvelles réglementations ou des modifications apportées aux lois existantes.

4.2.3 Peuvent contribuer aux mises à jour de politiques, aux audits ou au traitement d'une violation lorsque l'exposition juridique est en jeu.

[... 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 planifiée

9.1.1 La présente politique doit faire l'objet d'une revue tous les 12 mois par le DG.

9.1.2 La revue doit confirmer :

9.1.2.1 sa pertinence au regard du contexte juridique et contractuel en vigueur ;

9.1.2.2 la prise en compte adéquate des accords clients et des obligations de service ;

9.1.2.3 son alignement avec le registre de conformité et les autres politiques.

9.2 Mises à jour déclenchées par un événement

9.2.1 Une revue immédiate est requise si :

9.2.1.1 une nouvelle loi ou réglementation devient applicable (par ex. nouvelle règle relative à la protection des données) ;

9.2.1.2 un client ajoute des exigences de conformité complexes à son contrat ;

9.2.1.3 une violation ou un incident de non-conformité survient ;

9.2.1.4 l'entreprise étend ses activités à un nouveau marché ou à un secteur réglementé.

9.3 Approbation des mises à jour et gestion des versions

9.3.1 Toutes les mises à jour doivent être documentées, versionnées et approuvées par le DG.

9.3.2 Les versions historiques doivent être conservées à des fins d'audit et à des fins juridiques.

9.4 Communication des changements

9.4.1 Le personnel et les prestataires doivent être informés des changements de politique dans un délai de 5 jours ouvrés après approbation.

9.4.2 Tout fournisseur concerné doit également attester avoir pris connaissance des dispositions mises à jour avant de poursuivre la fourniture du service.

10. Politiques associées et articulations

10.1 La présente politique est appuyée et mise en œuvre au moyen des politiques PME suivantes :

10.1.1 P3S – Politique d'utilisation acceptable : prévient les comportements susceptibles d'enfreindre des exigences juridiques ou contractuelles (par ex. partage de fichiers non autorisé).

10.1.2 P8S – Politique de sensibilisation et de formation à la sécurité de l'information : sensibilise le personnel aux obligations de conformité et à la manière d'éviter les manquements.

10.1.3 P14S – Politique de conservation et d'élimination des données : garantit des pratiques licites de traitement des données tout au long de leur cycle de vie.

10.1.4 P17S – Politique de protection des données et de la vie privée : répond aux exigences du RGPD et des clients en matière de traitement des données.

10.1.5 P30S – Politique de réponse aux incidents : définit les modalités de réponse aux violations de données ou aux défaillances de conformité, y compris les délais de notification.

10.1.6 P36S – Politique relative aux médias sociaux et aux communications externes : garantit que les communications publiques n'enfreignent pas les obligations juridiques ou réglementaires.

10.2 Chaque politique liée met en œuvre une partie du dispositif de conformité juridique et doit être appliquée conjointement avec les autres.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1 – Actions à mettre en œuvre face aux risques et opportunités : inclut les risques de conformité.

11.1.2 Article 8.1 – Planification et maîtrise opérationnelles : exige l'exécution de processus respectant les exigences juridiques et contractuelles.

11.2 ISO/IEC 27002

11.2.1 Mesure 5.36 – Guide l'organisation dans la tenue des enregistrements d'obligations et dans la mise en place de réponses appropriées aux exigences juridiques et réglementaires.

11.3 NIST SP 800-53 Rév. 5

11.3.1 PL-1 – Politique et procédures : impose des politiques formelles de conformité.

11.3.2 PM-1 – Plan du programme de sécurité de l'information : exige l'intégration de la conformité juridique dans la planification de la sécurité.

11.3.3 CA-1 – Évaluation, autorisation et surveillance.

11.3.4 AU-1 – Politique d'audit : exige le maintien des éléments de preuve de conformité.

11.4 RGPD de l'UE

11.4.1 Article 5 – Principes relatifs au traitement des données, y compris la responsabilité.

11.4.2 Article 6 – Base légale du traitement.

11.4.3 Article 32 – Sécurité du traitement.

11.4.4 Article 33 – Notification d'une violation dans les 72 heures.

11.5 Directive NIS2 de l'UE

11.5.1 Article 21(2)(a) et (f) – Politiques internes relatives au risque et au contrôle réglementaire.

11.5.2 Article 23 – Application et sanctions en cas de défaillances de conformité.

11.6 Règlement DORA de l'UE

11.6.1 Article 5(2) – Supervision de la gestion des risques liés aux TIC.

11.6.2 Article 9(1) – Gouvernance interne de la conformité.

11.6.3 Article 17 – Dispositions contractuelles avec les prestataires de services TIC.

11.7 COBIT 2019

11.7.1 APO12 – Risques gérés : garantit que les risques de conformité sont suivis et traités.

11.7.2 APO13 – Sécurité gérée : couvre l'application fondée sur les risques de la conformité réglementaire et contractuelle.

11.7.3 DSS01 – Opérations gérées : impose une préparation opérationnelle permettant de satisfaire aux obligations légales.